Aspects arithmétiques et algorithmiques des courbes de genre 1, 2 et 3

Christophe Ritzenthaler

UNIVERSITÉ DE LA MÉDITERRANÉE AIX-MARSEILLE II

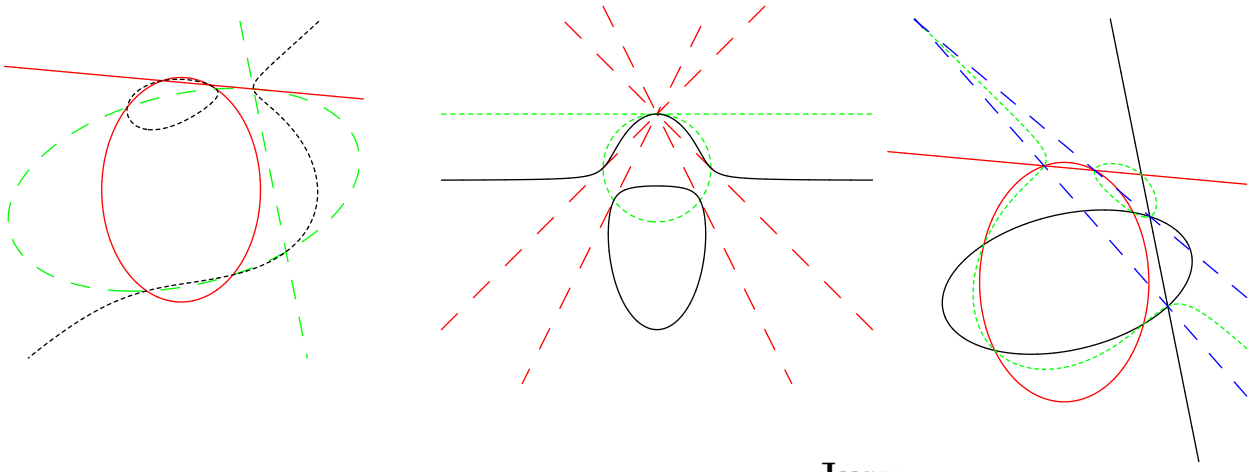
Institut de Mathématiques de Luminy

Habilitation à Diriger des Recherches
Spécialité : Mathématiques
présentée et soutenue publiquement par
Christophe Ritzenthaler
le 2 décembre 2009

Aspects arithmétiques et algorithmiques des courbes de genre $1, 2$ et 3

ou

à la rencontre du troisième genre : promenade mathématique à travers les courbes de genre 1, 2 et 3



Tuteur

M. Gilles Lachaud

Rapporteurs

M. Gerard van der Geer
Mme Kristin Lauter
M. Felipe Voloch

Jury

M. Noam D. Elkies
M. Gerard van der Geer
M. David Kohel
M. Gilles Lachaud
M. Jean-François Mestre
M. Enric Nart

Table des matières

Avant-propos

Ce mémoire d'habilitation est pour moi l'occasion de faire le point sur six années de recherche après ma thèse. J'ai effectué ce travail en partie à l'étranger, durant mes années de post-doctorat, et depuis 2006 au sein de l'équipe ATI à l'Institut de Mathématiques de Luminy, à Marseille. J'ai choisi de présenter dans ce mémoire mes travaux arithmétiques sur les courbes de genre 1, 2 et 3. Les quatre chapitres contenant ces résultats sont globalement indépendants. Ils peuvent ainsi être abordés dans l'ordre de préférence du lecteur. Par souci de cohérence, j'ai écarté de cette présentation les quatre articles [1], [5], [9] et [15].
Dans le premier chapitre, je développe divers aspects des quartiques planes en caractéristique 2. Les techniques utilisées sont souvent élémentaires car on manipule directement les objets. On peut ainsi se familiariser, de manière concrète, avec certaines méthodes et concepts (descentes, classes d'isogénie, invariants,...) qui seront réutilisées par la suite. Les deux chapitres suivants forment le cœur du mémoire et demandent plus de prérequis. Ils traitent respectivement de la caractérisation des classes d'isogénie de surfaces abéliennes sur un corps fini qui contiennent une jacobienne et des courbes maximales en genre 3. Enfin, le dernier chapitre, plus appliqué, concerne des problèmes d'origine cryptographique sur les courbes de genre $1, 2$ et 3. En tête de chaque chapitre, le lecteur trouvera une introduction au sujet concerné.

Nous avons souhaité rappeler un grand nombre de résultats, afin que le mémoire puisse se lire sans trop de références aux articles. Nous espérons que ceci en facilitera la lecture. S'il serait présomptueux d'écrire sur tant de sujets divers un état de l'art, j'espère que le lecteur y trouvera un outil de références. Les questions et les projets de recherche qui émaillent le mémoire sont autant d'invitations à prolonger l'ouvrage.

Notations et conventions pour l'ensemble de l'ouvrage. Chaque chapitre comporte plusieurs parties, elles-mêmes contenant des sections, divisées en paragraphes. On a harmonisé, autant que faire se peut, les notations. Celles-ci ne correspondent donc plus nécessairement à celles de l'article rapporté.
Les numéros [1],... (resp. [1'],...) correspondent aux articles et comptes-rendus publiés (resp. prépublications et travaux en cours) auquels j'ai pris part. Ils sont regroupés dans la partie 1.3. Les autres articles et préprints [Lan02],... sont regroupés en fin d'ouvrage.

L'entier q sera toujours la puissance $n > 0$ d'un premier p et k un corps fini de car-

dinal q. La lettre K désignera un corps quelconque. On notera $\mathbb{Z}_p$ l'anneau des entiers p-adiques, $\mathbb{Q}_p$ son corps des fractions, et v_p la valuation p-adique. Pour un entier $m > 0$, on notera également μ_m le groupe des racines de l'unité (pour un corps donné), S_m le groupe symétrique sur m éléments et D_{2m} le groupe diédral à $2m$ éléments.

On dira d'une propriété qu'elle est *géométrique* (ou parfois *absolue*) lorsqu'elle est vraie sur la clôture algébrique du corps. Sans précision supplémentaire, tout isomorphisme, automorphisme, etc. s'entendra défini sur le corps de base. On précisera par exemple $\bar{K}$-automorphisme, etc. si l'on veut parler géométriquement. Par abus, on dira souvent qu'une courbe est ordinaire, supersingulière, de p-rang a etc. si sa jacobienne a cette propriété.

Remerciements

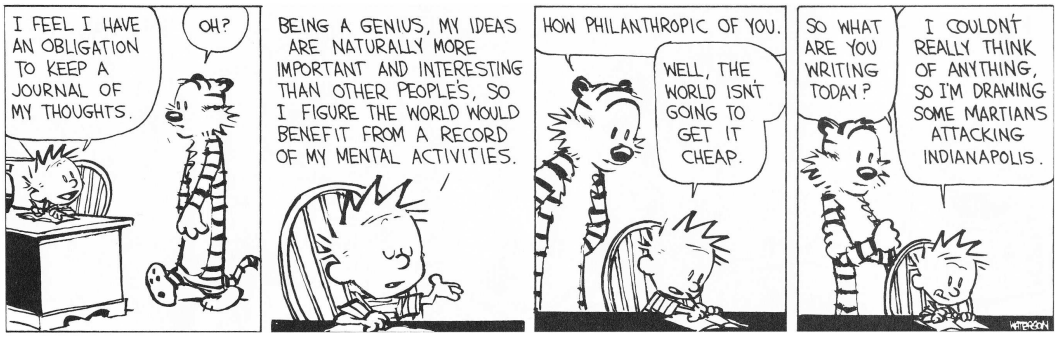
L'habilitation est un point culminant de plusieurs années de recherche. Ces remerciements vont tout naturellement à ceux, compagnons de cordées, guides, entraîneurs ou proches qui ont contribué directement ou indirectement à cette "ascension".

Ma gratitude va tout d'abord à mes rapporteurs, Gerard van der Geer, Kristin Lauter et Felipe Voloch, pour l'attention qu'ils ont bien voulu porter à ce mémoire et ce dans des délais très serrés et malgré leurs agendas bien remplis. Je remercie vivement les membres du jury qui me font l'amitié et l'honneur d'être présents à ma soutenance. Beaucoup d'entre eux ont été également des collaborateurs. C'est plus généralement tous ces derniers que je veux remercier : ils m'ont fait part de leurs idées, de leur savoir-faire en toute confiance et surtout m'ont fait découvrir le plaisir du travail en équipe. Les moments de partage d'une découverte sont les plus beaux de mes recherches. Parmi mes co-auteurs, je ne remercierai jamais assez Gilles Lachaud et Enric Nart, dont les apports à ma carrière et l'amitié dépassent largement nos multiples publications.

On entend parfois d'horribles histoires sur la vie de certains labos. Celui de l'IML doit faire exception car de nombreux collègues sont devenus des amis avec lesquels il fait bon discuter pendant les repas ou partir en voyage à l'autre bout du monde. Le travail à l'université est aussi facilité par l'efficacité et la bonne humeur des secrétaires (du labo et du département). Enfin, le jeune groupe des thésards contribue également à cette excellente atmosphère et à certaines soirées "legen... (wait for it)... dary".

Car il y a une vie en dehors du monde mathématique, merci à tous ceux qui l'ont rendue plus belle et passionnante. Ma famille, en particulier mes parents, pour leur soutien et leur amour indéfectibles, mes amis d'enfance et tous ceux que j'ai rencontrés de par le monde. Un grand merci à Magali pour sa relecture attentive des premières versions du mémoire et son soutien pendant la rédaction.

Och tack, lilla gumman, för våra passionerade och spännande år.



1 CV ET BIBLIOGRAPHIE PERSONNELLE

1.1 Notice individuelle

Christophe Ritzenthaler
Né le 4 janvier 1976 à Creutzwald (57)
Nationalité : française

Situation actuelle : Maître de conférences à l'université de la Méditerranée.

Adresse personnelle :
3, cours Jean Ballard
13001 Marseille
France

Tél. : 00 33 (0)4 91 33 59 40

Adresse professionnelle :
Institut de Mathématiques de Luminy
163 av. de Luminy Case 907
13288 Marseille
France
Tél. : 00 33 (0)4 91 26 95 84

E-mail : `ritzenth@iml.univ-mrs.fr`
Internet : `http://www.iml.univ-mrs.fr/~ritzenth/`

1.2 Formation

Sept. 1996	Entrée à l'École Normale Supérieure de Cachan.
1996-1997	Licence de Mathématiques à l'ENS de Cachan (mention **AB**).
1997-1998	Maîtrise de Mathématiques de l'Université Paris VII (mention **TB**). DEA Méthodes Algébriques de l'Université Paris VI (mention **B**).
1998-1999	Agrégation de Mathématiques (**rang 20**). Magistère de Mathématiques et d'Informatique de l'ENS Cachan et de l'université Paris 7 (mention Très honorable avec les Félicitations du jury).
1999-2003	Thèse sous la direction du Professeur Jean-François MESTRE, soutenue le 25 juin 2003 à l'Université Paris VII. *Titre :* Problèmes relatifs à certaines familles de courbes sur les corps finis. *Mention :* Très honorable. *Président :* Pr. Loïc MEREL Université Paris VII. *Rapporteurs :* Pr. Henri COHEN Université Bordeaux I. Pr. René SCHOOF Université Roma Tor Vergata. *Examinateurs :* Pr. Jean-Marc COUVEIGNES Université Toulouse II. Pr. François MORAIN École Polytechnique, Palaiseau
Sep. 2003 - Feb. 2004	Post-doctorat à l'IEM (Institut für Experimentelle Mathematik), Essen, Allemagne (Invité par Gerhard Frey, réseau GTEM).
Mars 2004 - Sep. 2004	Post-doctorat à l'institut de mathématiques de Leiden, Pays-Bas (Invité par Bas Edixhoven et Bart de Smit, réseau GTEM).
Octobre 2004	Invitation à l'université de Sydney, Australie (Invité par David Kohel).
Nov. 2004 - Aug. 2005	Post-doctorat à l'Universitat Autònoma de Barcelone, Espagne (invité par Enric Nart et Xavier Xarles, réseau AAG).
Sep. 2005	Invitation à l'université de Copenhague (DTU), Danemark (Invité par Tanja Lange).
Oct. 2005 - Dec. 2005	Invitation à l'université de Princeton, États-Unis (Invité par Manjul Bhargava).
Jan. 2006 -	Maître de conférences à l'université de la Méditerranée.

1.3 Références bibliographiques personnelles

Ces publications peuvent être trouvées à l'adresse suivante :

`http://www.iml.univ-mrs.fr/~ritzenth/research.html`

1.3.1 Articles et comptes-rendus

[1] Stéphane Ballet, Christophe Ritzenthaler et Robert Rolland : On the existence of dimension zero divisors for function fields over $\mathbb{F}_q$. À paraître dans Acta Arithmetica.

[2] Stéphane Flon, Roger Oyono et Christophe Ritzenthaler : Fast addition on non-hyperelliptic genus 3 curves. *In Algebraic geometry and its applications*, volume 5 de *Ser. Number Theory Appl.*, pages 1–28. World Sci. Publ., Hackensack, NJ, 2008.

[3] Steven D. Galbraith, Jordi Pujolàs, Christophe Ritzenthaler et Benjamin Smith : Distortion maps for supersingular genus two curves. *J. Math. Cryptol.*, 3(1):1–18, 2009.

[4] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler et A. Weng : The 2-adic CM method for genus 2 curves with application to cryptography. *In Advances in cryptology—ASIACRYPT 2006*, volume 4284 de *Lecture Notes in Comput. Sci.*, pages 114–129. Springer, Berlin, 2006. version Arxiv : `http://arxiv.org/abs/math/0503148`.

[5] M. Girard, D. Kohel et C. Ritzenthaler : The Weierstrass subgroup of a curve has maximal rank. *Bull. of London Math. Soc.*, 38:925–931, 2006.

[6] E. Howe, D. Maisner, E. Nart et C. Ritzenthaler : Principally polarizable isogeny classes of abelian surfaces over finite fields. *Math. Research Lett.*, 15:121–127, 2008.

[7] E. Howe, E. Nart et C. Ritzenthaler : Jacobians in isogeny classes of abelian surfaces over finite fields. *Annales de l'institut Fourier*, 59:239–289, 2009.

[8] Gilles Lachaud et Christophe Ritzenthaler : On some questions of Serre on abelian threefolds. *In Algebraic geometry and its applications*, volume 5 de *Ser. Number Theory Appl.*, pages 88–115. World Sci. Publ., Hackensack, NJ, 2008.

[9] D. Lehavi et C. Ritzenthaler : An explicit formula for the arithmetic geometric mean in genus 3. *Experimental Math.*, 16:421–440, 2007.

[10] J. Müller et C. Ritzenthaler : On the ring of invariants of ordinary quartic curves in characteristic 2. *J. of Algebra*, 303:530–542, 2006.

[11] E. Nart et C. Ritzenthaler : Non hyperelliptic curves of genus three over finite fields of characteristic two. *J. of Number Theory*, 116:443–473, 2006.

[12] E. Nart et C. Ritzenthaler : Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2. *Finite fields and their applications*, 14:676–702, 2008.

[13] E. Nart et C. Ritzenthaler : Genus three curves with many involutions and application to maximal curves in characteristic 2, 2010. à paraître dans les comptes-rendus de AGCT-12, http://arxiv.org/abs/0905.0546.

[14] Christophe Ritzenthaler : Automorphismes des courbes modulaires $X(n)$ en caractéristique p. *Manuscripta Math.*, 109(1):49–62, 2002.

[15] Christophe Ritzenthaler : Automorphism group of C: $y^3 + x^4 + 1 = 0$ in characteristic p. *JP J. Algebra Number Theory Appl.*, 4(3):621–623, 2004.

[16] Christophe Ritzenthaler : Point counting on genus 3 non hyperelliptic curves. *In Algorithmic number theory*, volume 3076 de *Lecture Notes in Comput. Sci.*, pages 379–394. Springer, Berlin, 2004.

1.3.2 Prépublications et travaux en cours

[1'] C. Arène, T. Lange, M. Naehrig et C. Ritzenthaler : Faster computation of Tate pairings, 2009. http://arxiv.org/abs/0904.0854.

[2'] Noam Elkies, Everett Howe et Christophe Ritzenthaler : Finiteness of the number of isogeny classes of Jacobians with factors in a finite set over finite fields.

[3'] Gilles Lachaud, Christophe Ritzenthaler et Alexey Zykin : Jacobians among abelian threefolds : a formula of Klein and a question of Serre, 2009. http://arxiv.org/abs/0802.4017.

[4'] Enric Nart et Christophe Ritzenthaler : A new proof of Weber's formula.

[5'] Christophe Ritzenthaler : A geometric approach of Serre's obstruction for genus 3 curve.

[6'] Christophe Ritzenthaler : *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. Thèse de doctorat, Université Paris VII, 2003.

[7'] Christophe Ritzenthaler : Explicit computations of Serre's obstruction for genus 3 curves and application to optimal curves, 2009. http://arxiv.org/abs/0901.2920.

1.3.3 Autres

Juil. 09. En collaboration avec G. Lachaud et M.A. Tsfasman, édition de *Arithmetic, Geometry, Cryptography and Coding Theory*, proceedings of AGC2T-11, CIRM (centre international de rencontres mathématiques), Marseille (France), November 5-9, 2007, Contemporary Math. **487**, (2009).

Sept. 08 - En collaboration avec E. Howe, K. Lauter and G. van der Geer, nous élaborons un site web dédié aux courbes optimales pour remplacer et compléter les tables disponibles sur http://www.science.uva.nl/~geer/. Ce site est disponible à l'adresse http://www.manypoints.org/

Mai 08. En collaboration avec R. Lercier, nous avons implémenté des algorithmes d'énumération des courbes de genre 2 sur les corps finis en MAGMA. En sous-routines, nous avons généralisé le calcul d'un modèle à partir des invariants en caractéristiques 2 et 3 et le calcul de toutes les tordues (pas uniquement quadratiques) en toute caractéristique. Ces programmes sont disponibles dans la version MAGMA 2.15, voir

`http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`

1.4 Activités d'encadrement et de formation à la recherche

Jan.08- Juin 09 Encadrement du mémoire de Master 2 de Marc Munsch sur les classes d'isogénie des variétés abéliennes en dimension 3.

Sept. 08 - Co-encadrement avec David Kohel de la thèse de Christophe Arène. Son sujet de thèse est décrit dans la section 5.2.3.

Jan 08 - Juin 08. Encadrement du mémoire de Master 2 de Christophe Arène sur les courbes d'Edwards. Ce mémoire a débouché sur l'écriture de l'article [1'].

Je co-anime également le groupe de travail pour les étudiants de thèse de l'équipe :

Sept. 2009 - Juin 2010	Géométrie algébrique et arithmétique, IML, Marseille.
Sept. 2008 - Juin 2009	Géométrie algébrique et arithmétique, IML, Marseille.
Dec. 2007 - Juin 2008	Multiplication complexe, IML, Marseille.
Sep. 2006 - Juin 2007	Surfaces algébriques, IML, Marseille.

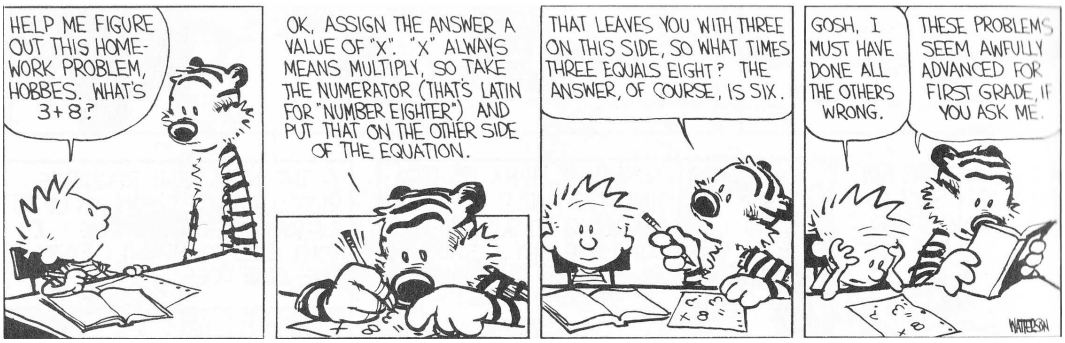
J'ai donné des cours à l'étranger pour des étudiants de M2 et post-doctorants. Ces cours sont disponibles à l'adresse

`http://iml.univ-mrs.fr/~ritzenth/enseignement.html`

Mai 2009. Cours de cryptographie de M2 sur les méthodes de comptages de points pour les courbes elliptiques (invitation de E. Gonzalez-Jimenez).

Septembre 2005. Sur l'invitation de T. Lange, j'ai effectué un cours introductif sur les méthodes p-adiques en cryptographie durant la semaine précédant la conférence E.C.C. à Copenhague.

Janvier 2005. Sur l'invitation de V. Rotger, j'ai effectué un cours de 20 heures à l'Universitat Politècnica de Barcelone. Ce cours constituait une introduction aux courbes sur les corps finis pour des étudiants en MASTER et comportait quatre parties : fonctions zêta (conjectures de Weil, théorie d'Honda-Tate), p-rang et applications ; automorphismes ; courbes maximales ; cryptographie. Il était accompagné de TD sur le logiciel MAGMA pour illustrer les différentes notions.



2 Quartique plane en caractéristique 2

Pourquoi étudier les quartiques planes en caractéristique 2 ? C'est d'abord le résultat d'une rencontre : d'un côté, l'étude par Enric Nart de certaines questions sur les courbes hyperelliptiques de genre 3 en caractéristique 2 ; de l'autre, la dernière partie de mon sujet de thèse, dédié au comptage des points sur les quartiques planes lisses en caractéristique 2. Depuis, les courbes de genre 3 en caractéristique 2 sont devenues le terrain de jeu qu'Enric et moi explorons au fil de nos rencontres. D'un point de vue plus mathématique, l'arithmétique et l'algorithmique des courbes de genre 3 sont la "nouvelle frontière" et constitue un challenge fascinant. En particulier, leur géométrie est distribuée dans le plan et non plus concentrée sur la droite, ce qui rend leur combinatoire très riche.

En genre 1 et 2, la caractéristique 2 est un cas particulier. Les quartiques ne dérogent pas à la règle et il est donc indispensable de leur réserver un traitement à part. Cependant, contrairement au cas des genres 1 et 2, la caractéristique 2 est relativement plus facile que les autres et ceci en raison de l'existence de bons modèles géométriques découverts par Wall. Ainsi, la description des isomorphismes étant simple sur ces modèles, nous avons pu mener à bien un procédé classique de descente. Il en a résulté la description de modèles arithmétiques, des groupes d'automorphismes, le dénombrement des classes d'isomorphismes sur $\mathbb{F}_{2^n}$ et le calcul du nombre de points de l'espace des modules associé. Ceci est exposé dans la partie 2.1. Par la suite avec Müller, nous avons réalisé dans le cas ordinaire (qui est le cas générique) le calcul d'un système complet d'invariants. À cette époque, un tel système pour les quartiques n'était même pas connu sur $\mathbb{C}$ et seul un système d'invariants primaires, dû à Dixmier, était explicite (depuis, les travaux de Ohno ont permis d'exhiber un tel système). Les résultats principaux de nos travaux sont rappelés dans la partie 2.2. Des applications arithmétiques sont également issues du travail sur les modèles. En connection avec le problème de Serre (voir le chapitre 4), Nart et moi avons utilisé plusieurs familles de modèles pour construire des courbes optimales de genre 3 sur $k = \mathbb{F}_{2^n}$ (rappelons qu'une courbe est dite *optimale* lorsque son nombre de points atteint la borne de Serre-Weil). Pour n pair, en utilisant les modèles supersinguliers, on montre que des courbes optimales existent dès que $n \geq 6$ et peuvent être construites explicitement. En fait, on répond plus généralement au problème de la caractérisation des classes d'isogénie des variétés abéliennes supersingulières de dimension 3 sur k qui contiennent une jacobienne. Ceci fait l'objet de la partie 2.3. Dans le cas où n est impair, des courbes optimales sont obtenues pour une infinité de valeurs de n.

On travaille pour cela avec des quartiques ayant beaucoup d'involutions. C'est le sujet de la partie 2.4.
Enfin, on pourra se reporter à la partie 2.5 pour les nombreuses questions qui restent ouvertes en caractéristique quelconque et quelques pistes pour les étudier.

Notations et conventions pour le chapitre. On notera $k = \mathbb{F}_{2^n} = \mathbb{F}_q$ un corps fini de caractéristique 2 et de cardinal q, k_m l'extension (dans une clôture algébrique donnée) de k de degré m, $\mathrm{AS}(k) = \{x + x^2,\ x \in k\}$ et $r_0 \in k \setminus \mathrm{AS}(k)$ un élément fixe. On prendra $r_0 = 1$ si n est impair. Par "quartique" on entendra "quartique plane".

2.1 Modèles des quartiques en caractéristique 2

Cette partie se rapporte à l'article [11] avec Enric Nart.

Toute courbe (lisse, projective, absolument irréductible) non hyperelliptique de genre 3 se plonge canoniquement dans $\mathbb{P}^2$ comme une quartique (plane) lisse. Inversement toute quartique lisse est une courbe de genre 3 non hyperelliptique. Or, la description d'une quartique requiert 15 coefficients (en projectif) alors que l'espace des modules des courbes de genre 3, noté M_3, est de dimension 6. Peut-on atteindre ce nombre minimal de paramètres ? La rationalité de $\mathsf{M}_3(\mathbb{C})$ démontrée par [Kat96] montre qu'un tel modèle existe mais on n'en connaît pas explicitement. Pourtant, la description de telles courbes est importante autant du point de vue théorique que calculatoire. Nous reviendrons sur cette question dans la partie 2.5 en général. Mais pour l'instant, en caractéristique 2, la question est résolue de manière satisfaisante par le résultat suivant, puisqu'un polynôme homogène de degré 2 est décrit par 6 paramètres.

Théorème 2.1.1 ([Wal95, Prop.1])**.** *Soit K un corps algébriquement clos de caractéristique 2. Toute quartique sur K est isomorphe à une quartique de la forme $Q^2 = r$ où $Q(x, y, z) \in K[x, y, z]$ est un polynôme homogène de degré 2 et $r(x, y, z)$ est de la forme*

$$xyz(x + y + z),\ xyz(y + z),\ xy(y^2 + xz),\ x(y^3 + x^2z)$$

ou

$$x^2yz,\ x^3y,\ 0.$$

Les trois derniers cas ne nous intéressent pas car ils ne donnent que des quartiques singulières. Chacun des quatre premiers cas, lorsque la courbe est lisse, a un nombre bien défini de *bitangentes* (c'est-à-dire de droites tangentes à la quartique en deux points (distincts ou non)) :

1. 7 dans le premier cas : $\{x, y, z, x + y, x + z, y + z, x + y + z\}$;
2. 4 dans le deuxième : $\{x, y, z, y + z\}$;
3. 2 dans le troisième : $\{x, y\}$;
4. et une seule dans le quatrième cas : $\{x\}$.

Par [SV87, p.60], nous savons que ceci reflète le 2-rang de la jacobienne de la courbe lorsque celle-ci est lisse, c.-à-d. 3 dans le premier cas (cas *ordinaire*), 2 dans le deuxième cas, 1 dans le troisième et 0 dans le quatrième. Dans cette partie, motivés par des applications arithmétiques, on donne des familles de modèles sur un corps fini k de caractéristique 2. Les résultats de l'article [11] étant assez dispersés, nous allons rappeler ici, de manière synthétique, les principaux résultats. Nous mettrons en particulier en avant la présentation des modèles rationnels et des groupes d'automorphismes. On a parfois reformulé certains des résultats de *loc. cit.* dans cette optique. Remarquons que les applications étant pour les corps finis, nous nous limitons à ce cas, même si certains résultats sont vrais plus généralement.

Notations et conventions pour la partie. Pour alléger les notations, on notera par $'$ la conjugaison $x \mapsto x^q$, qu'on étendra aux polynômes par action sur leurs coefficients. Pour un corps K, on note $\mathcal{Q}(K)$ l'ensemble des formes quadratiques ternaires

$$Q(x, y, z) = ax^2 + by^2 + cz^2 + dxy + eyz + fzx,$$

à coefficients dans K.

2.1.1 Idées générales des démonstrations

On utilise la théorie de la descente, comme énoncée dans [Ser68, §4.20] dans le cas particulier des variétés projectives. Rappelons-en le principe car celui-ci est utilisé à maintes reprises dans différents chapitres. Soient donc V'/K' une variété projective sur un corps K' et K un sous-corps de K' tel que K'/K soit une extension galoisienne finie. "Descendre V' de K' à K" signifie qu'il existe une variété V/K et un K'-isomorphisme $f : V \to V'$. Si tel est le cas, pour tout $\sigma \in \mathrm{Gal}(K'/K)$, on définit le K'-isomorphisme $h_\sigma = f^\sigma \circ f^{-1} : V' \to V'^\sigma$. Ces K'-isomorphismes satisfont à la relation de cocycle

$$h_{\sigma\tau} = h_\sigma^\tau h_\tau, \quad \forall \sigma, \tau \in \mathrm{Gal}(K'/K). \tag{2.1}$$

Inversement supposons que pour tout $\sigma \in \mathrm{Gal}(K'/K)$ il existe des K'-isomorphismes de V' dans V'^σ satisfaisant (2.1). [Ser68, §4.Prop.12] montre alors que la descente de V' de K' à K est possible et qu'elle est unique à K-isomorphisme près.
Dans ce chapitre, nous aurons besoin de cette proposition dans le cas d'une courbe sur $\bar{K}$ qu'on souhaite descendre sur un corps fini $K = \mathbb{F}_q$. On peut alors reformuler la condition comme suit. Étant donnée une courbe C' sur $\bar{K}$, une *donnée de descente* sur K est fournie par un isomorphisme $\gamma : C' \to C'^\sigma$ tel que

$$\gamma^{\sigma^{m-1}} \circ \cdots \circ \gamma^\sigma \circ \gamma = 1 \tag{2.2}$$

pour un certain $m \geq 1$ et $\sigma : x \mapsto x^q$ l'automorphisme de Frobenius de $\mathrm{Gal}(\bar{K}/K)$. A (C', γ) on peut associer une unique courbe C/K à K-isomorphisme près et un $\bar{K}$-isomorphisme $\phi : C \to C'$ tel que $\gamma = \phi^\sigma \circ \phi^{-1}$.

Une notion proche est la notion de tordue (ou forme) comme énoncée dans [Ser94, Chap.3.1.3] (voir aussi [Sil92, X.§.2] dans le cas des courbes). Soit V une variété sur un corps K et K'/K une extension galoisienne. On dit qu'un variété V'/K est une K'/K-*tordue* de V (ou simplement une tordue de V si $K' = K^{\text{sep}}$) si V et V' sont K'-isomorphes. On montre alors classiquement qu'on peut définir une injection de l'ensemble des K'/K-tordues de V dans $H^1(\text{Gal}(K'/K), \text{Aut}_{K'}(V))$. Si de plus V est projective, cette application est une bijection. Ainsi, seules les variétés qui possèdent des $\bar{K}$-automorphismes ont des tordues.

Remarque 2.1.2. Dans le cas d'une courbe C sur un corps fini, [vdGvdV92b, Cor.5.2] montre que si $\text{Aut}(C) = \{1\}$ alors la courbe n'a pas de tordue.

Pour les quartiques sur k, nous pouvons appliquer la théorie de la descente de manière systématique car les isomorphismes entre deux modèles des familles du théorème 2.1.1 sont particulièrement simples. Dans le cas ordinaire par exemple, les isomorphismes entre les modèles

$$Q^2 = xyz(x + y + z), \quad Q \in \mathcal{Q}(\bar{k})$$

doivent préserver l'ensemble des 7 bitangentes. Ils sont donc tous donnés projectivement par des éléments de $\Gamma = \text{PGL}_3(\mathbb{F}_2)$ (et pas seulement de $\text{PGL}_3(\bar{\mathbb{F}}_2)$). La relation (2.2) devient ainsi une condition d'ordre sur γ et les données de descente ne dépendent que des classes de conjugaison des éléments. Des résultats similaires sont exploités dans les autres cas. Il "suffit" alors de deviner pour chaque donnée de descente un bon modèle sur k, le plus souvent en fixant une action galoisienne transitive sur l'ensemble des bitangentes. Les groupes d'automorphismes sont quant à eux décrits comme l'ensemble des éléments stabilisateurs [11, Lem.1.6]. La connaissance de ces derniers et l'utilisation de la formule dite des orbites permettent alors de calculer le nombre de classes d'isomorphisme de quartiques sur k.

2.1.2 Le cas ordinaire

Proposition 2.1.3 ([11, Th.1.8])**.** *L'ensemble $\mathcal{C}_k$ des classes d'isomorphisme des quartiques lisses ordinaires sur k se scinde en six familles correspondant aux classes de conjugaison des éléments de Γ*

$$\mathcal{C}_k = \mathcal{C}_1 \amalg \mathcal{C}_2 \amalg \mathcal{C}_3 \amalg \mathcal{C}_4 \amalg \mathcal{C}_{7,0} \amalg \mathcal{C}_{7,1},$$

où le premier indice indique le degré minimal de l'extension sur laquelle sont définies les bitangentes.

Par des arguments combinatoires, on obtient le résultat suivant.

Théorème 2.1.4 ([11, Th.1.9])**.** *Il y a $q^6 - q^5 + q^4 - 3q^3 + 5q^2 - 6q + 7$ classes d'isomorphisme de quartiques lisses ordinaires sur $\mathbb{F}_q$. Plus précisément, elles se répartissent de la manière suivante*

$\mathcal{C}_1$	$\frac{1}{168}\left(q^6 - 7q^5 + 42q^4 - 140q^3 + 343q^2 - 462q + 328\right)$
$\mathcal{C}_2$	$\frac{1}{8}\left(q^6 - 3q^5 + 6q^4 - 12q^3 + 15q^2 - 6q\right)$
$\mathcal{C}_3$	$\frac{1}{3}\left(q^6 - q^5 - 2q^3 + 4q^2 - 6q + 7\right)$
$\mathcal{C}_4$	$\frac{1}{4}\left(q^6 - q^5 - q^2 - 2q + 4\right)$
$\mathcal{C}_{7,0} \cup \mathcal{C}_{7,1}$	$\frac{1}{7}(q^6 + 6) + \frac{1}{7}(q^6 + 6)$

Pour chacune des familles nous allons donner des modèles ainsi que les possibles groupes d'automorphismes sur k.

Famille $\mathcal{C}_1$

Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = xyz(x + y + z), \quad Q \in \mathcal{Q}(k),$$

avec les conditions de lissité

$$abc \neq 0,\ a + b + d \neq 0,\ b + c + e \neq 0,\ a + c + f \neq 0 \text{ et } a + b + c + d + e + f \neq 1. \quad (2.3)$$

Pour toute courbe C_Q dans cette famille, on a $\mathrm{Aut}(C_Q) = \mathrm{Aut}_{\bar{k}}(C_Q)$. Les groupes d'automorphismes sont donnés dans [Wal95, p.411] (on note Dim. la dimension du lieu dans l'espace des modules des courbes de genre 3, noté M_3) :

Groupe	Générateurs	Conditions	Dim.
$\{1\}$			6
$\mathbb{Z}/2\mathbb{Z}$	$(x : z : y)$	$d = f,\ b = c$	4
$\mathbb{Z}/2\mathbb{Z}$	$(x : y : x + z)$	$c = f,\ e = 1$	4
$(\mathbb{Z}/2\mathbb{Z})^2$	$(x : x + y : z)$ et $(x : y : x + z)$	$b = d,\ c = f,\ e = 1,\ d \neq f$	3
H_8	$(x : z : y)$ et $(x : y : x + z)$	$b = c = d = f,\ e = 1,\ (a, d) \neq (0, 0)$	2
S_3	$(x : y : y + z)$ et $(x : z : y)$	$d = f = 1,\ b = c = e,\ a \neq 1,\ b \neq 1$	2
S_4	stabilisateur de $(1 : 0 : 0)$ dans $\mathrm{PGL}_3(\mathbb{F}_2)$	$a = d = f = 1,\ b = c = e,\ a \neq b$	1
S_4	stabilisateur de $x = 0$ dans $\mathrm{PGL}_3(\mathbb{F}_2)$	$b = c = d = e = f = 1$ et $a \neq 1$	1
$\mathrm{PGL}_3(\mathbb{F}_2)$		$a = b = c = d = e = f = 1$	0

On a noté H_8 le groupe des quaternions d'ordre 8, S_n le groupe symétrique sur n éléments et $(l_1 : l_2 : l_3)$ l'automorphisme $(x : y : z) \mapsto (l_1 : l_2 : l_3)$.

Famille $\mathcal{C}_2$

Soit $u \in k_2 \setminus k$ une solution de $u^2 + u = r_0$. Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = (r_0x^2 + ry^2 + xy)z(x + y + z), \quad Q \in \mathcal{Q}(k)$$

avec les conditions de lissité

$$c \neq 0,\ a+b+d \neq 0,\ a+b+c+d+e+f \neq 1, Q(u,u',0) \neq 0 \text{ et } Q(u,u',1) \neq 0.$$

Les groupes d'automorphismes non triviaux de C_Q sont donnés dans [11, p.458].

Groupe	Générateurs	Conditions
$\mathbb{Z}/2\mathbb{Z}$	$(y:x:z)$	$a=b,\ e=f,\ f\neq c,\ d\neq 1$
$\mathbb{Z}/2\mathbb{Z}$	$(y:x:x+y+z)$	$e=f=a+b+c,\ a\neq b$
$\mathbb{Z}/2\mathbb{Z}$	$(x:y:x+y+z)$	$c=e=f,\ a\neq b$
$\mathbb{Z}/2\mathbb{Z}$	$(y+z:x+z:z)$	$a=b,\ d+e+f=1,\ e\neq f$
$\mathbb{Z}/2\mathbb{Z}$	$(x+z:y+z:z)$	$a=b+e+f,\ d=1,\ e\neq f$
$(\mathbb{Z}/2\mathbb{Z})^2$	$(y:x:z)$ et $(x:y:x+y+z)$	$a=b,\ c=e=f,\ d\neq 1$
$(\mathbb{Z}/2\mathbb{Z})^2$	$(y:x:z)$ et $(x+z:y+z:z)$	$a=b,\ d=1,\ e=f\neq c$
D_8	$(y:x:z),(x:y:x+y+z),$ $(x+z:y+z:x+y+z)$	$a=b,\ d=1,\ c=e=f$

On a noté D_8 le groupe diédral à 8 éléments.

Famille $\mathcal{C}_3$

Soient $s \in k$ tel que $f(x)=x^3+x^2+s$ soit irréductible et $v \in k_3 \setminus k$ une solution de $f(x)=0$. Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = \ell\ell'\ell''(x+y+z),\ Q \in \mathcal{Q}(k) \text{ et } \ell = vx+v'y+v''z,$$

avec les conditions de lissité

$$Q(v,v',v'') \neq 0, Q(v+1,v'+1,v''+1) \neq 0, Q(1,1,1) \neq 1.$$

Le groupe des automorphismes de C_Q est trivial sauf si $a=b=c$ et $d=e=f$, où il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et engendré par $(y:z:x)$ (cf. [11, p.458]).

Famille $\mathcal{C}_4$

Soient $t \in k$ tel que $t^{-1} \notin \mathrm{AS}(k)$ et $w \in k_4 \setminus k_2$ une solution de

$$w^4+(t+t^2)w^2+t^2w=1.$$

Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = \ell\ell'\ell''\ell''',\ Q \in \mathcal{Q}(k) \text{ et } \ell = wx+w'y+w''z,$$

avec les conditions de lissité

$$Q(w+t+1,w+w',w'+1) \neq 0, Q(w+w',t,w'+w'') \neq 0 \text{ et } Q(1,0,1) \neq t^2.$$

D'après [11, p.459], le groupe des automorphismes de C_Q est trivial sauf si

1. $a=c$ et $d+e+f=0$ ($f\neq 0$ ou $b\neq c$), auquel cas il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et engendré par $(y+z:x+y+z:x+z)$;
2. $a=b=c$, $f=0$ et $d=e$, auquel cas il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et engendré par $(z:x+z:y+z)$.

Familles $\mathcal{C}_{7,0}$ et $\mathcal{C}_{7,1}$

D'après le lemme [11, Lem.1.11], tout polynôme irréductible P sur k divisant le polynôme $(x^{q^3-1}+x^{q-1}+1)$ (cas 0) ou le polynôme $x^{q^3-1}+x^{q^2-1}+1$ (cas 1) est de degré 7. Par exemple, on peut prendre pour P le polynôme x^7+x+1 pour le cas 0 (resp. le cas 1) si $n \equiv 1,2,4 \pmod 7$ (resp. $n \equiv 3,5,6 \pmod 7$) (N.B. : la remarque correspondante dans notre article est incorrecte). Soit $i = 0,1$ et $\zeta \in k_7 \setminus k$ une racine de P dans le cas i. Tout élément de la famille $\mathcal{C}_{7,i}$ est k-isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = \ell\ell'\ell''(\ell+\ell'+\ell''), \quad Q \in \mathcal{Q}(k_7) \text{ et } \ell = (\zeta x + \zeta' y + \zeta'' z)$$

avec la condition de rationalité $Q + Q' = \ell \cdot \ell'$ et la condition de lissité $Q(p) \neq 0$ où p est le point d'intersection de $\ell = 0$ et $\ell' = 0$.
Le groupe des automorphismes de C_Q est trivial sauf si C est une tordue de la courbe de Klein [11, p.461] :

$$C : x^2y^2 + y^2z^2 + x^3z + xy^3 + xz^3 + yz^3 = 0 \quad \text{(cas 0)},$$

ou

$$C : x^4 + y^4 + z^4 + x^3z + xy^3 + xyz^2 + yz^3 = 0 \quad \text{(cas 1)}.$$

Dans ces cas, le groupe des automorphismes est isomorphe à $\mathbb{Z}/7\mathbb{Z}$ et il est engendré par $(z : x+z : y)$ dans le cas 0 et $(z : x : y+z)$ dans le cas 1.

2.1.3 Le cas de 2-rang 2

Théorème 2.1.5. *Il y a $q^5-q^4+q^3-2q^2+2q-1$ classes d'isomorphisme de quartiques lisses de 2-rang 2 sur $\mathbb{F}_q$. Elles se répartissent en les trois classes $\mathcal{C}_i$ suivantes selon le degré i minimal de l'extension sur laquelle sont définies leurs quatre bitangentes*

$\mathcal{C}_1$	$\frac{1}{6}\left(q^5-3q^4+6q^3-7q^2+5q-2\right)$
$\mathcal{C}_2$	$\frac{1}{2}\left(q^5-q^4-q^2+q\right)$
$\mathcal{C}_3$	$\frac{1}{3}\left(q^5-q^2+2q-2\right)$

Famille $\mathcal{C}_1$

Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = xyz(y+z), \quad Q \in \mathcal{Q}(k)$$

avec $b = 1$ et les conditions de lissité $ac \neq 0$ et $c + e \neq 1$. Pour toute courbe C_Q dans la famille, on a $\mathrm{Aut}(C_Q) = \mathrm{Aut}_{\bar{k}}(C_Q)$. Ils sont donnés dans [11, p.464] et ci-dessous.

Groupe	Générateurs	Condition	Dim.
$\{1\}$		$b = 1$	5
$\mathbb{Z}/2\mathbb{Z}$	$(x : y + z : z)$	$b = e = 1$, $d = 0$, $f \neq 0$ ou $c \neq 1$	3
$\mathbb{Z}/2\mathbb{Z}$	$(x : z : y)$	$b = c = 1$, $d = f$, $f \neq 0$ ou $e \neq 1$	3
$\mathbb{Z}/2\mathbb{Z}$	$(x : y : y + z)$	$b = 1$, $c = e$, $f = 0$, $d \neq 0$ ou $c \neq 1$	3
S_3	$(x : y + z : z)$, $(x : z : y)$	$b = c = e = 1$, $d = f = 0$	1

Remarque 2.1.6. Le cas C_3 de [Wal95, p.411] n'existe pas. Les conditions données dans notre article pour les cas $\mathbb{Z}/2\mathbb{Z}$ sont légèrement erronées.

Famille $\mathcal{C}_2$

Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = xy(r_0y^2 + yz + z^2), \quad Q \in \mathcal{Q}(k)$$

avec $b = 1$ et les conditions de lissité $a \neq 0$ et $(1, e) \neq (cr, c)$.
Le groupe d'automorphismes de C_Q est trivial sauf si $c = e$ et $f = 0$, auquel cas il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et engendré par $(x : y : y + z)$.

Famille $\mathcal{C}_3$

Soit $s \in k^*$ tel que le polynôme $x^3 + x + s$ soit irréductible. Soit alors $t \in k$ une solution de l'équation $t^2 + t + 1 = s^{-1}$. Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$C_Q : Q^2 = x(y^3 + ty^2z + (t + 1)yz^2 + z^3), \quad Q \in \mathcal{Q}(k)$$

avec $b = 1$ et les conditions de lissité $a \neq 0$ et $(c, e) \neq (0, 0)$.
Le groupe d'automorphismes de C_Q est trivial sauf si $c = e = 1$ et $d = f = 0$ auquel cas il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et engendré par $(x : z : y + z)$.

2.1.4 Le cas de 2-rang 1

D'après le théorème 2.1.1, toute quartique lisse de 2-rang 1 est $\bar{k}$-isomorphe à une quartique de la famille

$$Q^2 = xy(y^2 + xz), \quad Q \in \mathcal{Q}(\bar{k})$$

avec $a = 1$, $d = 0$ et la condition de lissité $c \neq 0$. Il s'agit d'une famille de dimension 4. Les groupes de $\bar{k}$-automorphismes sont tous triviaux sauf si $f \neq 0$ et $e = cf^{-2}$ (dimension 3) pour lequel il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et engendré par $(x : y : z + f^{-2}y)$.

Remarque 2.1.7. Dans [Wal95, p.412], il y a une coquille pour le cas C_2 : l'automorphisme est $(x : y : z + f^{-2}y)$. De plus le cas C_3 est toujours singulier.

On montre ensuite [11, Prop.2.3] que toute quartique lisse de 2-rang 1 a ses deux bitangentes définies sur le corps k et que la descente est triviale. Néanmoins, l'action des isomorphismes est plus complexe ce qui amène à considérer deux familles de même modèle mais dont les paramètres décrivent des ensembles distincts.

Théorème 2.1.8. *Il y a $q^4 - 2q^2 + q$ classes d'isomorphismes de quartiques lisses de 2-rang 1 sur $\mathbb{F}_q$. Elles se répartissent en deux familles : $\mathcal{C}_1$ avec $(q-1)^2q(q+1)$ classes et $\mathcal{C}_2$ avec $(q-1)q^2$ classes.*

Famille $\mathcal{C}_1$

Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$Q^2 = xy(y^2 + xz), \quad Q \in \mathcal{Q}(k)$$

avec $a \in k^*/(k^*)^3$, $f \neq 0$, $d \in \{0, f^{-1}r_0\}$ et la condition de lissité $c \neq 0$.

Remarque 2.1.9. Dans notre article, la condition $f \neq 0$ n'est pas signalée.

Tous les groupes d'automorphismes sont triviaux sauf si $e = cf^{-2}$ pour lequel le groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et engendré par $(x : y : z + f^{-2}y)$.

Famille $\mathcal{C}_2$

Tout élément de la famille est isomorphe à une courbe C_Q de la forme

$$Q^2 = xy(y^2 + xz), \quad Q \in \mathcal{Q}(k)$$

avec $a \in k^*/(k^*)^3$, $d = f = 0$ et la condition de lissité $c \neq 0$. Tous les groupes d'automorphismes sont triviaux.

2.1.5 Le cas de 2-rang 0

Ces quartiques lisses admettant une unique bitangente, celle-ci est définie sur le corps de base. On montre à nouveau [11, Prop.2.4] que la descente est triviale. Dans les cas précédents, le polygone de Newton de la jacobienne était entièrement déterminé par le 2-rang (c'est vrai aussi en caractéristique différente de 2). Cependant et contrairement au cas de genre 1 et 2, une courbe de 2-rang 0 n'est pas nécessairement supersingulière. D'après [WM71], les pentes dans ce cas sont soit $\frac{1}{2}$ et la courbe est supersingulière, soit $\frac{1}{3}$ puis $\frac{2}{3}$. On appellera ce dernier cas *type* $\frac{1}{3}$. Puisque la pente des polygones de Newton des courbes elliptiques et des surfaces abéliennes de p-rang 0 est $\frac{1}{2}$, la jacobienne d'une courbe de type $\frac{1}{3}$ est absolument simple.

Théorème 2.1.10 ([11, Prop.2.5])**.** *Toute quartique lisse C sur k est isomorphe à une courbe d'une des deux familles suivantes*

$$\mathcal{N}: \qquad Q^2 = x(y^3 + x^2z), \qquad Q = (a, b, c, 0, e, 0),\ c \in k^*/(k^*)^9,\ a, b \in k,\ e \in k^*,$$

ou

$$\mathcal{S}: \qquad Q^2 = x(y^3 + x^2z), \qquad Q = (a, 0, c, d, 0, f),\ c \in k^*/(k^*)^9,\ a, d, f \in k.$$

De plus C est supersingulière (resp. de type $\frac{1}{3}$) si et seulement si C appartient à la famille $\mathcal{S}$ (resp. à $\mathcal{N}$). Il y a $2q^2 - q + [4q-2]_{q\equiv 1 \pmod 3} + [6]_{q\equiv 1 \pmod 9}$ (resp. $(q-1)q^2$) classes d'isomorphisme dans la famille $\mathcal{S}$ (resp. $\mathcal{N}$). La notation $[a]_{condition}$ signifie que a doit être ajouté si la condition est satisfaite.

Il est de plus remarquable que le groupe des $\bar{k}$-automorphismes des éléments de la famille $\mathcal{N}$ sont tous triviaux alors que ceux de la famille $\mathcal{S}$ ne le sont jamais (ce fait est essentiel dans la démonstration du théorème précédent). Plus précisément, on note $E_{c,f} : k \to k$ l'homorphisme $\mathbb{F}_2$-linéaire $E_{c,f}(x) = cx^2 + fx + \sqrt{x}$ et

$$\gamma_{t,v}(x : y : z) = (t^3 x : t^{-1} y : t^{-9}(z + vx)).$$

Les automorphismes sont de la forme $\gamma_{t,v}$ où les paramètres t, v sont donnés dans le tableau ci-dessous.

(t, v)	Condition	Dim.
$t = 1$, $v \in \ker(E_{c,f})$	$d \neq 0$	3
$t \in \mu_3(k)$ $v \in \ker(E_{c,f})$	$d = 0$, $f \neq 0$	2
$\{t \in \mu_3(k), v \in \ker(E_{c,f})\}$ II $\{t \in \mu_9(k) \setminus \mu_3(k)$, $v \in \{E_{c,0}^{-1}(t^3 a) \cap k\}\}$	$d = f = 0$	1

Remarque 2.1.11. Dans le cas $d = f = 0$, Nart m'a indiqué que

$$Aut_{\bar{k}}(C) \simeq \mu_9(\bar{k}) \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}).$$

2.1.6 Résultats globaux

En utilisant les résultats obtenus dans [NS04] pour le cas hyperelliptique et le résultat de [Oor91a] démontrant qu'il n'existe pas de courbes hyperelliptiques de genre 3 supersingulières en caractéristique 2, on obtient le résultat suivant.

Proposition 2.1.12 ([11, Cor.3.2])**.** *Il y a*

$$q^6 + 2q^5 + q^4 + q^3 + q^2 + q + 2 - [4q - 2]_{q \equiv -1 \pmod 3} + [6]_{q \equiv 1 \pmod 9} + [12]_{q \equiv 1 \pmod 7}$$

classes d'isomorphisme de courbes de genre 3 *définies sur* $\mathbb{F}_q$*. En fonction du polygone de Newton de leur jacobienne, elles sont réparties ainsi :*

ordinaire	$q^6 + q^5 - q^4 - q^3 + q^2 - 4q + 7$
2-*rang* 2	$q^5 + q^4 - 3q^3 + q^2 + q - 1$
2-*rang* 1	$q^4 + 4q^3 - 4q^2 + q - 2$
type 1/3	$q^3 + q^2 + [12]_{q \equiv 1 \pmod 7}$
supersingulière	$2q^2 - q + [4q - 2]_{q \equiv 1 \pmod 3} + [6]_{q \equiv 1 \pmod 9}$

On souhaite calculer le nombre de classes de $\bar{k}$-isomorphismes de certaines courbes de genre 3 sur k, c.-à-d. le nombre de points k-rationnels sur l'espace des modules grossier associé M. D'après [vdGvdV92b, Prop.5.1], pour toute courbe C/k, on a

$$\sum_{C'} \# \operatorname{Aut}(C')^{-1} = 1,$$

la somme étant prise sur un ensemble de représentants C' des classes d'isomorphismes de tordues de C. Ainsi

$$\sum_{C\in\text{classes d'iso.}} \frac{1}{\mathrm{Aut}(C)} = \sum_{\substack{C\in\text{classes}\\ \text{de } \bar{k}-\text{iso.}}} \sum_{\substack{C'\in\text{tordues}\\ \text{de } C}} \frac{1}{\mathrm{Aut}(C')} = \sum_{\substack{C\in\text{classes}\\ \text{de } \bar{k}-\text{iso.}}} 1 = \#\mathsf{M}(k).$$

D'autre part si $\mathcal{C}$ est une famille de courbes et que les classes d'isomorphisme sont données par l'action d'un groupe fini G sur $\mathcal{C}$, la formule des orbites donne

$$\sum_{\substack{C\in\text{classes d'iso.}\\ \text{de la famille } \mathcal{C}}} \frac{1}{\mathrm{Aut}(C)} = \frac{\#\mathcal{C}}{\#G}.$$

La connaissance des familles décrites dans cette partie et de leur groupe d'automorphisme fournit ainsi le résultat suivant.

Théorème 2.1.13 ([11, Th.3.4])**.** *On note M_3^{nh} (resp. M_3^h) le lieu non hyperelliptique (resp. hyperelliptique) de l'espace des modules des courbes de genre 3, M_3. Le nombre de points $\mathbb{F}_q$-rationnels sur les différents lieux de M_3^{nh}, M_3^h et M_3 pour le polygone de Newton est donné par*

	ordinaire	2-*rang* 2	2-*rang* 1	*type* 1/3	*supersingulière*
M_3^{nh}	q^6-q^5+1	q^5-q^4	q^4-q^3	q^3-q^2	q^2
M_3^h	q^5-q^4	$q^4-2q^3+q^2$	$2(q^3-q^2)$	q^2	*0*
M_3	q^6-q^4+1	$q^5-2q^3+q^2$	$q^4+q^3-2q^2$	q^3	q^2

En particulier $\#\mathsf{M}_3(\mathbb{F}_q) = q^6+q^5+1$. Ce résultat, conjecturé par Brock et Granville en toute caractéristique [BG01], a été démontré par Bergström [Ber01].

2.2 Invariants des quartiques lisses ordinaires en caractéristique 2

Cette partie est basée sur l'article [10] avec Jürgen Müller.

2.2.1 Quelques notions sur les invariants

Soit $R = \bigoplus_{d\geq 0} R_d$ une algèbre commutative $\mathbb{N}$-graduée de type fini sur un corps K, telle que $\dim_K(R_d) < \infty$ pour $d > 0$ et $R_0 \cong K$. On note $R_+ := \bigoplus_{d>0} R_d \lhd R$.

Définition 2.2.1. Un ensemble $\mathcal{F} = \{f_1, \ldots, f_m\} \subset R_+$ d'éléments homogènes avec $m = \dim(R)$, la dimension de Krull de R, est appelé un *système homogène de paramètres* si $\mathcal{F}$ est algébriquement indépendant et si R est un $K[\mathcal{F}]$-module de type fini.

Avec nos hypothèses sur R, un système homogène de paramètres existe toujours. On définit les invariants dans le contexte suivant.

Soit V un K-espace vectoriel de dimension finie et G un groupe réductif agissant sur V par une représentation linéaire rationnelle. On note $K[V]$ l'anneau des polynômes vu comme anneau des fonctions régulières de la variété affine V et

$$R = K[V]^G = \{f \in K[V] \mid f(\sigma^{-1} \cdot x) = f(x) \text{ pour tout } \sigma \in G, x \in V\},$$

l'anneau des *G-invariants* de V. Puisque G est supposé réductif, R est de type fini. De plus si G est fini, $\dim(R) = \dim_K(V)$.

Définition 2.2.2. Un système homogène de paramètres $\mathcal{F}$ de R est appelé un ensemble (ou système) *d'invariants primaires*. Un ensemble minimal de générateurs homogènes du $K[\mathcal{F}]$-module R est appelé un ensemble (ou système) *d'invariants secondaires*. On dira d'un système d'invariants qu'il est *complet* s'il engendre la K-algèbre R.

La connaissance d'un système d'invariants est d'une grande utilité, aussi bien théorique que pratique, en géométrie algébrique. On pourra consulter [Dix87] pour une jolie introduction sur le sujet. Illustrons simplement notre propos avec le cas des courbes hyperelliptiques car ceci nous sera utile pour la partie 5.4.
Soit K un corps algébriquement clos. Pour $r \geq 1$ et $m \geq 1$, notons $R^{(r,m)}$ l'anneau des invariants pour l'action naturelle du groupe réductif $\mathrm{SL}_r(K)$ sur le K-espace vectoriel des r-formes de degré m. Par l'action des racines r-ièmes de l'unité, on voit facilement que $R_s^{(r,m)} = \{0\}$ si $sm \not\equiv 0 \pmod r$. Ainsi si I est un invariant homogène de degré s non nul, on définit son *poids* ω par sm/r.
Considérons des courbes hyperelliptiques C_1, C_2 sur K de caractéristique différente de 2, d'équation $C_i : z^{m-2}y^2 = f_i(x, z)$ avec les f_i des formes binaires homogènes de même degré m. Ces courbes sont isomorphes si et seulement si

$$f_1(x, z) = \lambda f_2(ax + bz, cx + dz) \text{ pour } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(K) \text{ et } \lambda \in K.$$

Si $I \in R_s^{(2,m)}$ est un invariant homogène de degré s, alors $I(f_1) = \lambda^s I(f_2) = I(\lambda f_2)$. Inversement, supposons qu'il existe un $\lambda \in K$ tel que l'égalité précédente soit satisfaite pour un système complet d'invariants de $R^{(2,m)}$. Si on note X l'ouvert des formes binaires de degré m sans racines multiples alors $X \mapsto X /\!\!/ \mathrm{SL}_2(K)$ est un quotient géométrique, c.-à-d. deux éléments de X sont dans la même $\mathrm{SL}_2(K)$-orbite si et seulement si tous leurs invariants sont égaux. Comme les f_i sont sans racines multiples, cela implique l'égalité $f_1 = \lambda f_2 \circ M$ avec $M \in \mathrm{SL}_2(K)$ et donc les courbes C_i sont isomorphes. Si $m = 4$, cela correspond au cas des courbes de genre 1. Lorsque $K = \mathbb{C}$, l'anneau $R^{(2,4)}$ est un anneau de polynômes à deux indéterminées I, J explicites de degré 2 et 3 [Aro50]. En particulier $I^3/(I^3 - 27J^2)$ est le j-invariant de la courbe elliptique associée. Plus généralement, on appelle *invariant absolu* le quotient de deux invariants homogènes de même degré. Cette notion est importante puisque les invariants absolus sont des fonctions sur l'espace des modules associé et donnent des informations sur un corps de définition minimal de l'objet. Pour $m = 6$, c.-à-d. en genre 2, plusieurs systèmes co-existent pour des raisons historiques et pratiques (pire, les notations ne sont jamais vraiment fixes) :

– Les invariants de Clebsch A, B, C, D de degré $2, 4, 6, 10$ et R de degré 15 [Mes91a, p.317] tel que R^2 est un polynôme en A, B, C, D. Ces invariants sont complets en caractéristique différente de 2 ;
– Les invariants absolus

$$i_1 = A^5/D, i_2 = A^3B/D \text{ et } i_3 = A^2C/D.$$

Clebsch et Bolza ont montré que lorsque $A \neq 0$, les courbes C_i sont isomorphes sur $\mathbb{C}$ si et seulement si leurs invariants i_1, i_2, i_3 sont égaux. L'implication directe est évidente. Considérons la réciproque. Posons $A(f_1)/A(f_2) = \lambda^2 \in \mathbb{C}$. Alors puisque $i_m(f_1) = i_m(f_2)$ on a

$$D(f_1) = \lambda^{10}D(f_2), \quad B(f_1) = \lambda^4 B(f_2), \quad C(f_1) = \lambda^6 B(f_2).$$

Comme R^2 est un polynômes de degré 15 en A, B, C, D, on a $R(f_1)^2 = \lambda^{30}R(f_2)^2$. Ceci implique que $R(f_1) = (\pm\lambda)^{15}R(f_2)$. Les autres invariants sont de degré pair, on peut remplacer λ par $\pm\lambda$ et on a l'égalité souhaitée pour tous les invariants. Ceci montre également que $\mathsf{M}_2 \otimes \mathbb{C}$ est rationnel puisque son corps des fonctions est $\mathbb{C}(i_1, i_2, i_3)$;
– Les invariants d'Igusa–Clebsch A', B', C', D', R de même degré que les précédents [Mes91a, p.319] ;
– Les invariants d'Igusa $J_2, J_4, J_6, J_8, J_{10}$ [Mes91a, p.324]. Ceux-ci forment ce qu'on appelle un *système d'invariants entiers* au sens de [Igu60]. En particuliers ils forment un système complet d'invariants en toute caractéristique. Ceci permet à Igusa de donner une description explicite de l'anneau N tel que $\operatorname{Spec} N$ soit le schéma des modules des courbes de genre 2 [Mes91a, p.325]. On notera également j_1, j_2, j_3 les invariants absolus d'Igusa définis en caractéristique 0 par

$$j_1 = J_4J_6/J_{10}, \quad j_2 = J_2^3J_4/J_{10} \text{ et } j_3 = J_2^2J_6/J_{10}.$$

– Les invariants absolus de Cardona-Quer-Nart-Pujolàs g_1, g_2, g_3 dont la définition est différente en caractéristique 2 [CNP05, Sec.2.1] et différente de 2 [CQ05]. Nous les avons introduits avec Reynald Lercier pour notre programme de reconstruction des courbes de genre 2 et de leurs tordues (voir la section 2.5.2). Leur définition, qui se décline en plusieurs cas, est motivée par le souci de couvrir toutes les éventualités (caractéristique ou annulation de certains invariants). Ils sont définis comme suit en fonction des invariants d'Igusa.

1. Si la caractéristique du corps est 2 et $J_2 \neq 0$ alors

$$(g_1, g_2, g_3) = \left(\sqrt{J_{10}/J_2^5}, \sqrt{(J_8/J_2^4) - (J_4/J_2^2)^4 - (J_4/J_2^2)^3}, \sqrt{J_4/J_2^2}\right).$$

Si $J_2 = 0$ et $J_6 \neq 0$ alors

$$(g_1, g_2, g_3) = \left(0, \sqrt{J_{10}^3/J_6^5}, \sqrt[8]{J_8J_{10}^4/J_6^8}\right).$$

Enfin si $J_2 = J_6 = 0$ alors $(g_1, g_2, g_3) = (0, 0, \sqrt[8]{J_8^5/J_{10}^4})$.

2. Si la caractéristique du corps est différente de 2 et si $J_2 \neq 0$ alors

$$(g_1, g_2, g_3) = (J_2^5/J_{10}, J_2^3 J_4/J_{10}, J_2^2 J_6/J_{10}).$$

Si $J_2 = 0$ et $J_4 \neq 0$ alors $(g_1, g_2, g_3) = (0, J_4^5/J_{10}^2, J_4 J_6/J_{10})$.
Enfin, si $J_2 = J_4 = 0$ alors $(g_1, g_2, g_3) = (0, 0, J_6^5/J_{10}^3)$.

Ainsi, sans aucune restriction, deux courbes de genre 2 sur un corps K sont $\bar{K}$-isomorphes si et seulement si leurs invariants absolus (g_1, g_2, g_3) sont égaux.

En genre 3 on rencontre deux cas : le cas hyperelliptique et le cas des quartiques lisses. Pour le premier, Shioda [Shi67] a déterminé explicitement sur $\mathbb{C}$ un système de 9 invariants soumis à 5 relations pour $R^{(2,8)}$. Tout récemment le cas de $R^{(2,7)}$ a lui aussi été résolu [Bed07]. On reviendra sur des questions liées au cas hyperelliptique dans la partie 2.5.

Passons au cas non hyperelliptique. Dans *loc. cit.*, Shioda calcule également la série de Hilbert $H_{R^{(3,4)}}(t) = \sum_{d=0}^{\infty} \dim_{\mathbb{C}}(R_d^{(3,4)}) t^d$ de $R^{(3,4)}$ sur $\mathbb{C}$

$$H_{R^{(3,4)}}(t) = \frac{D(t)}{(1-z^3)(1-z^6)(1-z^9)(1-z^{12})(1-z^{15})(1-z^{18})(1-z^{27})}$$

avec

$$\begin{aligned} D(t) = 1 + z^9 + z^{12} + 2z^{18} + 3z^{21} + 2z^{24} + 3z^{27} + 4z^{30} + 3z^{33} + 4z^{36} + 4z^{39} \\ + 3z^{42} + 4z^{45} + 3z^{48} + 2z^{51} + 3z^{54} + 2z^{57} + z^{60} + z^{63} + z^{66} + z^{75}. \end{aligned}$$

Les algèbres $R^{(r,m)}$ étant Cohen-Macaulay par le théorème de Hochster-Roberts [DK02, Th.2.5.5], $R^{(3,4)}$ peut être engendrée par au plus $D(1) + 3 = 56$ éléments de degré au plus 75 (le "3" prevenant de la contribution des invariants primaires de degré $3, 6, 15$). Shioda conjecturait que $R^{(3,4)}$ pouvait être engendrée par 13 éléments seulement. Par la suite, Dixmier [Dix87] a exhibé sur $\mathbb{C}$ un ensemble de 7 invariants primaires de degré $\{3, 6, 9, 12, 15, 18, 27\}$. Les invariants secondaires étaient quant à eux inconnus. Dans ce contexte, Jürgen Müller et moi-même avons considéré le problème de la détermination d'un système complet d'invariants en caractéristique 2 pour les quartiques lisses ordinaires (celles-ci forment un ouvert dans l'espace des modules M_3). Une des motivations étaient de tester la conjecture grâce aux résultats obtenus.

Remarque 2.2.3. Depuis notre travail, la conjecture de Shioda est acquise par les calculs de Ohno (voir [GK06]). Ce dernier a explicité six invariants secondaires qui engendrent avec ceux de Dixmier l'anneau $R^{(3,4)}$.

Dans le chapitre 4, nous aurons besoin de l'invariant primaire de degré 27 qui n'est autre que le *discriminant* de la quartique. Plus généralement, lorsque r, m sont quelconques, rappelons la définition du discriminant sur un corps K algébriquement clos de caractéristique première à m (voir [Lan02, p.397], [GKZ94, Chap.9]). Soit F la r-forme de degré m générique et $q_1, \ldots, q_r$ ses dérivées partielles. Le discriminant de F est

$$\operatorname{Disc} F = c_{r,m}^{-1} \cdot \operatorname{Res}(q_1, \ldots, q_n), \quad c_{r,m} = m^{((m-1)^r - (-1)^r)/m}$$

où $\mathrm{Res}(q_1, \ldots, q_n)$ est le discriminant multivarié uniformisé comme dans [GKZ94, p.426]. Si $r = 3$ et K est de caractéristique 0, cet invariant est un polynôme irréductible sur $\mathbb{Z}$ de degré $3(m-1)^2$ et de poids $m(m-1)^2$. Il est nul si et seulement si la courbe plane définie par $F = 0$ est singulière. Si $r = 2$ et K de caractéristique 0, il coïncide avec le discriminant univarié usuel au signe près, c.-à-d. si

$$F(x, z) = \sum a_i x^i z^{n-i} = z^n \cdot f(x/z)$$

alors $\mathrm{Disc}(F) = \mathrm{Res}_x(f(x), f'(x))/a_n$.

Exemple 2.2.4. Dans le cas $r = 3$ et $m = 4$, le discriminant est un invariant de degré 27 et de poids 36. Il existe une jolie formule due à Sylvester pour le calculer (voir [GKZ94, p.118] pour une présentation moderne). De plus dans le cas particulier où

$$f(x, y, z) = a_1 x^4 + a_2 y^4 + a_3 z^4 + 2(b_1 y^2 z^2 + b_2 x^2 z^2 + b_3 x^2 y^2),$$

on a

$$\mathrm{Disc}\, f = 2^{40}\, a_1\, a_2\, a_3\, (c_1\, c_2\, c_3)^2\, \det(M)^4,$$

où

$$M = \begin{bmatrix} a_1 & b_3 & b_2 \\ b_3 & a_2 & b_1 \\ b_2 & b_1 & a_3 \end{bmatrix} \in \mathrm{Sym}_3(k),$$

et pour $1 \leq i \leq 3$, les $c_i = a_j a_k - b_i^2$ sont les cofacteurs des a_i. On renvoie à [8, Sec.2.2] pour une démonstration de cette formule. Notons cependant que la constante diffère légèrement car l'uniformisation par $c_{3,4} = 2^{14}$ n'est pas utilisée dans cet article.

Après cette longue disgression, nous allons maintenant passer aux résultats de l'article.

2.2.2 Résultats

Comme nous l'avons vu dans la section 2.1.1, l'étude des classes de $\bar{k}$-isomorphismes des quartiques lisses ordinaires est simplifiée par le fait qu'elles peuvent être décrite par l'action du groupe *fini* $\Gamma = \mathrm{PGL}_3(\mathbb{F}_2)$ sur la famille $Q^2 = xyz(x + y + z)$. Pour rendre l'action linéaire et plus simple, on change le modèle en $Q^2 = C$ où

$$C = x^4 + y^4 + z^4 + (xy)^2 + (yz)^2 + (zx)^2 + x^2yz + xy^2z + xyz^2$$

est l'équation d'une tordue de la quartique de Klein $x^3y + y^3z + z^3x = 0$. En particulier C est invariante par l'action de Γ (c'est en fait l'invariant de Dickson de degré 4 sous l'action de Γ). Notons W' (noté W'^* dans l'article) le Γ-module $\mathbb{F}_2[a, b, c, d, e, f]$ avec l'action naturelle de Γ sur les coniques

$$Q = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$$

de $\mathbb{P}^2$. On pose $R = \mathbb{F}_2[a, b, c, d, e, f]^\Gamma = W'^\Gamma$, l'anneau des invariants. Comme Γ est un groupe fini, les invariants séparent les orbites [DK02, p.53], et on obtient le résultat suivant.

Théorème 2.2.5 ([11, Prop.1.4],[10, Prop.2.5]). *Le lieu des quartiques lisses ordinaires dans* $\mathsf{M}_3 \otimes \bar{k}$ *est isomorphe à l'ouvert explicite (donné par les conditions de lissité* (2.3)*) de la variété affine* $\mathrm{Spec}(R) \otimes \bar{k}$.

Avec l'action très naturelle de Γ, il est surprenant que le calcul des invariants résiste (ait résisté ?) aux algorithmes généralistes de logiciels tels que MAGMA ou GAP. Plus précisément, si le calcul des invariants primaires est relativement rapide, celui des invariants secondaires semblait hors de portée. Ceci est dû principalement au fait que nous sommes dans le cas *modulaire*, c.-à-d. la caractéristique du corps divise l'ordre du groupe. La seconde partie de l'article [10] consiste alors à trouver des techniques spécifiques pour le calcul des invariants. Décrivons brièvement les différentes étapes du raisonnement.

On calcule tout d'abord la série de Hilbert de R. On ne peut utiliser directement les résultats standards car nous sommes dans le cas modulaire. On procède donc comme suit. W' est un facteur direct d'un Γ-module de permutation explicite W (noté W^* dans l'article). Rappelons qu'un module de permutation est un module qui admet une base permutée par l'action du groupe. D'après [Ben98, Cor.3.11.4] on peut relever W' et W sur $\mathbb{Z}_2$ en des $\mathbb{Z}_2[\Gamma]$-modules $\tilde{W}'$ et $\tilde{W}$ et on a la relation $H_R(t) = H_{\mathbb{Q}_2[\tilde{W}' \otimes \mathbb{Q}_2]^\Gamma}(t)$ [DK02, Prop.3.10.15]. Le calcul de cette série de Hilbert s'effectue alors de manière classique grâce au théorème de Molien [Ben93, Th.2.5.2] et on trouve [10, Prop.4.2]

$$H_R(t) = \frac{1+t^4+2t^5+t^6+t^7+t^8+2t^9+2t^{10}+t^{11}+t^{12}+t^{13}+2t^{14}+t^{15}+t^{19}}{(1-t^2)\cdot(1-t^3)^2\cdot(1-t^4)\cdot(1-t^6)\cdot(1-t^7)}.$$

On montre ensuite que R est Cohen-Macaulay (ceci n'est pas automatique dans le cas modulaire). Soit $D \subset \Gamma$ un sous-groupe de 2-Sylow d'ordre 8. En utilisant les techniques standards implantées dans MAGMA on calcule $R' = \mathbb{F}_2[W']^D$. R' est Cohen-Macaulay, il est facile d'en déduire [10, Prop.4.3] que R l'est aussi. Grâce à cette propriété et à la connaissance de la série de Hilbert, on sait combien d'invariants chercher et leur degré. La décomposition $W = W' \oplus \mathbb{F}_2$ permet de trouver très aisément les invariants primaires en utilisant le fait que W est un module de permutation [10, Sec.4.4]. On obtient même un ensemble dit *optimal* d'invariants primaires (c.-à-d. dont le produit des degrés est minimal parmi les systèmes d'invariants primaires) de degré $\{2,3,3,4,6,7\}$. Pour les invariants secondaires, on met en place une méthode itérative, en générant une liste d'invariants de bon degré. On s'assure que le système devient complet grâce à une condition d'indépendance linéaire dans le $\mathbb{F}_2$-espace vectoriel $R'/\mathcal{F}'R'_+$ où $\mathcal{F}'$ est un ensemble d'invariants primaires de R' [10, Sec.4.4]. Les calculs sont menés grâce à un programme spécifique en MAGMA (`http://iml.univ-mrs.fr/~ritzenth/programme/invariant.mag`). On trouve 18 invariants secondaires dont les 6 premiers (de degré $\{0,4,5,5,6,7\}$) ajoutés aux invariants primaires engendrent l'algèbre R. Ce calcul prend moins d'une minute.

2.3 Variétés abéliennes supersingulières de dimension 3 sur $\mathbb{F}_{2^n}$

Dans cette partie, on décrit les résultats de [12] avec Enric Nart.

Étant donnés un entier $g \geq 0$ et un corps fini quelconque $K = \mathbb{F}_\ell$ un problème fameux et très étudié consiste à trouver quel est le nombre maximal de points des courbes (lisses, absolument irréductibles, projectives) de genre g sur K. Nous renvoyons le lecteur au chapitre 4 pour un aperçu du problème. Rappelons simplement qu'on note $N_\ell(g)$ le nombre maximal de points d'une telle courbe et que la borne de Serre-Weil montre que $N_\ell(g) \leq 1 + \ell + gm$ où $m = \lfloor 2\sqrt{\ell} \rfloor$. On dira qu'une courbe est *maximale* lorsque son nombre de points rationnels est $N_\ell(g)$ et *optimale* lorsque son nombre de points rationnels atteint la borne de Serre-Weil. On considère aussi parfois des courbes *minimales*, c.-à-d. celles dont le nombre de points rationnels atteint la borne inférieure $1 + \ell - gm$.

Remarque 2.3.1. Les définitions ne sont pas "symétriques" : à l'opposée d'optimal, on pourrait introduire *infimal*. Cependant l'intérêt pour les courbes minimales étant moindre et comme nous n'aurons pas besoin de cette distinction ici, nous conservons la dénomination classique de minimal.

On se restreint maintenant au cas $\ell = q = 2^n$ et $g = 3$. Après l'étude dans [11] des modèles (Sec. 2.1) et les résultats en genre 2 de [MN07] (voir Chap. 3), il nous a paru naturel d'étudier les classes d'isogénie des variétés abéliennes de dimension 3 supersingulières sur k et plus précisément de répondre à la question analogue au genre 2, c.-à-d. la caractérisation des classes contenant une jacobienne. De plus, lorsque q est un carré, il est facile de voir que les courbes optimales et minimales sont supersingulières. Ainsi, une des conséquences de notre étude est la démonstration de l'existence de courbes optimales et minimales sur $\mathbb{F}_{2^n}$ pour tous les $n > 6$ pairs (les cas $n = 2, 4, 6$ sont également résolus). Les résultats sont explicites comme nous le verrons brièvement dans la section 2.3.3.

L'étude se déroule en trois temps. Grâce aux automorphismes des courbes supersingulières, on trouve explicitement la décomposition à isogénie près de la jacobienne de ces courbes en produit de courbes elliptiques. Ceci permet d'exprimer la classe d'isogénie de la jacobienne comme un produit de restrictions de Weil de courbes elliptiques supersingulières. Dans un second temps, on écrit les classes possibles pour les variétés abéliennes supersingulières de dimension 3 sur k et on les compare à celles ci-dessus. Finalement, on montre que pour q assez grand, ces dernières contiennent toujours une jacobienne. Pour cela, on démontre qu'à partir des coefficients des différentes courbes elliptiques, on peut reconstruire une courbe de genre 3.

2.3.1 "Démontage" des courbes de genre 3 supersingulières

L'article [Oor91a] démontrant qu'il n'existe pas de courbe hyperelliptique de genre 3 supersingulière en caractéristique 2, on se concentre sur les quartiques (planes) lisses supersingulières, ce qui correspond à la famille $\mathcal{S}$ du théorème 2.1.10. Un changement de variables (on pose $z = \sqrt{c}Y$, $x = 1$, $y = X$) et de notations pour les paramètres permettent de se ramener aux notations de l'article [12], c.-à-d.

$$C : Y^4 + fY^2 + gY = X^3 + dX^2 + e, \quad g \in k^*, d, e, f \in k. \tag{2.4}$$

Avec cette écriture, le groupe des $\bar{k}$-automorphismes de C admet un sous-groupe de la forme $(\mathbb{Z}/2\mathbb{Z})^2$ engendré par les involutions

$$i_\theta(X, Y) = (X, Y + \nu)$$

où θ parcourt les trois racines non nulles $\theta_1, \theta_2, \theta_3$ de $Y^4 + fY^2 + gY = 0$ dans $\bar{k}$. Les quotients de C par ces trois involutions s'écrivent

$$C/\langle i_\theta \rangle \simeq E_\theta : y^2 + y = a_\theta x^3 + a_\theta d x^2 + a_\theta e, \quad a_\theta = (g^{-1}\theta)^2. \tag{2.5}$$

On dira que C est de *type réductible*, (resp. *type quadratique*, *type cubique*) suivant que le nombre des racines θ rationnelles est 3, (resp. 1, 0). Si E/k_m, on notera $\mathrm{Res}_{k_m/k}(E)$ la restriction de Weil de E à k. C'est une variété abélienne de dimension m.

Lemme 2.3.2 ([12, Lem.3.2])**.** *Si C est de type cubique alors sa jacobienne J est isogène à $\mathrm{Res}_{k_3/k}(E_{\theta_i})$ pour un $i \in \{1, 2, 3\}$ quelconque. Si C est de type quadratique avec $\theta_1 \in k$ alors J est isogène à $E_{\theta_1} \times \mathrm{Res}_{k_2/k}(E_{\theta_2})$. Si C est de type réductible alors J est isogène à $E_{\theta_1} \times E_{\theta_2} \times E_{\theta_3}$.*

Dans un second temps, il s'agit d'écrire quelles sont les classes d'isogénie des variétés abéliennes de dimension 3 supersingulières et de les comparer avec les classes du lemme 2.3.2.

2.3.2 Classes d'isogénie sur $k = \mathbb{F}_{2^n}$

Pour les variétés abéliennes de dimension 3 supersingulières

Une variété abélienne de dimension 3 supersingulière sur k est soit simple, soit le produit d'une courbe elliptique supersingulière et d'une surface abélienne supersingulière simple, soit le produit de trois courbes elliptiques supersingulières. On rappelle les classes d'isogénie possibles pour ces objets.

Soient les courbes elliptiques supersingulières suivantes :

$$\begin{array}{lll} E_a: & y^2 + y = ax^3, & a \in k^*, \\ H: & y^2 + y = x^3 + x^2, & \\ E_0: & y^2 + y = c_0^{-3}x^3 + x^2, & c_0 \in k \setminus \mathrm{AS}(k). \end{array}$$

On note E' la tordue quadratique d'une courbe elliptique E et (E, t) le couple formée de la courbe et de sa trace. On couvre les classes d'isogénie de polynôme de Weil $x^2 - tx + q$ de la manière suivante

– si n est pair,

$$(E_1, (-1)^{n/2}2\sqrt{q}),\ (E_1', -(-1)^{n/2}2\sqrt{q}),\ (E_a, -(-1)^{n/2}\sqrt{q}),\ (E_a', (-1)^{n/2}\sqrt{q}),$$

et $(E_0, 0)$ avec $a \in k^*$ qui n'est pas un cube dans k.

– si n est impair,

$$(E_1, 0),\ (H, -(-1)^{(n^2-1)/8}\sqrt{2q}) \text{ et } (H', (-1)^{(n^2-1)/8}\sqrt{2q}).$$

Pour les classes d'isogénie des surfaces abéliennes supersingulières simples, on note $A_{a,b}$ une surface abélienne dans la classe d'isogénie de polynôme de Weil

$$x^4 + ax^3 + bx^2aqx + q^2.$$

D'après la référence [MN02, Th.2.9] (voir aussi Th.3.1.2)

– si n est pair,

$$A_{(0,0)},\ A_{(0,-q)},\ A_{(\sqrt{q},q)} \text{ et } A_{(-\sqrt{q},q)};$$

– si n est impair,

$$A_{(0,-2q)},\ A_{(0,q)},\ A_{(0,-q)},\ A_{(\sqrt{2q},q)} \text{ et } A_{(-\sqrt{2q},q)}.$$

Enfin, une application directe de la théorie de Honda-Tate nous donne les variétés de dimension 3 supersingulières simples [12, Prop.2.1] : si n est impair, il n'en existe pas ; si n est pair, leur polynôme de Weil est $x^6 \pm q^{3/2}x^3 + q^3$.

Remarque 2.3.3. Dans l'article, il est écrit (de manière erronée) $x^6 \pm \sqrt{q}x^3 + q^3$.

Classes obtenues par restriction de Weil

Rappelons simplement les résultats de l'article [12, Sec.3].

– Lorsque n est pair, on note $\epsilon = (-1)^{n/2}$ et E_{nc} une courbe E_a avec a qui n'est pas un cube.

E/k_3	Polynôme de Weil de $\mathrm{Res}_{k_3/k} E$	classe d'isogénie de
E_0	$x^6 + q^3$	$E_0 \times A_{(0,-q)}$
E_1	$x^6 - 2\epsilon\sqrt{q^3}x^3 + q^3$	$E_1 \times E_{nc} \times E_{nc}$
E'_1	$x^6 + 2\epsilon\sqrt{q^3}x^3 + q^3$	$E'_1 \times E'_{nc} \times E'_{nc}$
E_{nc}, E'_{nc}	$x^6 \pm \sqrt{q^3}x^3 + q^3$	simple

E/k_2	Polynôme de Weil de $\mathrm{Res}_{k_2/k} E$	classe d'isogénie de
E_0	$x^4 + q^2$	$A_{(0,0)}$
E_1	$x^4 - 2qx^2 + q^2$	$E_1 \times E'_1$
E'_1	$x^4 + 2qx^2 + q^2$	$E_0 \times E_0$
E_{nc}	$x^4 + qx^2 + q^2$	$E_{nc} \times E'_{nc}$
E'_{nc}	$x^4 - qx^2 + q^2$	$A_{(0,-q)}$

– Lorsque n est impair, on note $\epsilon = (-1)^{(n^2-1)/8}$.

E/k_3	Polynôme de Weil de $\mathrm{Res}_{k_3/k} E$	classe d'isogénie de
E_1	$x^6 + q^3$	$E_1 \times A_{(0,-q)}$
H	$x^6 - \epsilon\sqrt{2q^3}x^3 + q^3$	$H \times A_{(-\epsilon\sqrt{2q},q)}$
H'	$x^6 + \epsilon\sqrt{2q^3}x^3 + q^3$	$H' \times A_{(\epsilon\sqrt{2q},q)}$

E/k_2	Polynôme de Weil de $\mathrm{Res}_{k_2/k} E$	classe d'isogénie de
E_0	$x^4 + q^2$	$H \times H'$
E_1	$x^4 + 2qx^2 + q^2$	$E_1 \times E_1$
E_1'	$x^4 - 2qx^2 + q^2$	$A_{(0,-2q)}$
E_{nc}	$x^4 - qx^2 + q^2$	$A_{(0,-q)}$
E_{nc}'	$x^4 + qx^2 + q^2$	$A_{(0,q)}$

2.3.3 Jacobiennes et courbes optimales

En observant les tableaux de la section 2.3.2, on voit que certaines classes sont exclues.

Proposition 2.3.4 ([12, Prop.3.3])**.** *Soit A une variété abélienne supersingulière sur k de dimension 3. Il n'y a pas de jacobienne isogène à A dans les cas suivants*

- *pour n pair : A est isogène à $E \times A_{(\pm\sqrt{q},q)}$ pour toute courbe elliptique supersingulière E sur k.*
- *pour n impair : A est isogène à $E_1 \times A_{(\pm\sqrt{2q},q)}$ ou $H \times A_{(\epsilon\sqrt{2q},q)}$ ou $H' \times A_{(-\epsilon\sqrt{2q},q)}$, avec $\epsilon = (-1)^{(n^2-1)/8}$.*

Plus étonnant, lorsque $n > 6$, cette condition nécessaire est également suffisante comme le montre le résultat principal de l'article.

Théorème 2.3.5 ([12, Th.3.6,3.7,3.8])**.** *On note f le polynôme de Weil d'une courbe elliptique supersingulière sur k, g celui d'une surface abélienne supersingulière sur k et h le produit de trois polynômes de Weil de courbes elliptiques supersingulières sur k. Les entiers ϵ prennent ici toutes les valeurs ± 1.*

- *Toute les classes d'isogénie de variétés abéliennes supersingulières simples de dimension 3 contiennent une jacobienne.*
- *Les classes d'isogénie de polynôme de Weil fg contiennent une jacobienne à l'exception des cas suivants :*
  - *Si $q = 2$, $g(x) = x^4 - 4x^2 + 4$ ou*

    $$f(x)g(x) = (x^2+\epsilon 2x+2)(x^4-\epsilon 2x^2+4), \quad (x^2+2x+2)(x^4-2x^3+2x^2-2x+4);$$

  - *Si $q = 4$,*

    $$f(x)g(x) = (x^2+4)(x^4+16), \quad (x^2 \pm 4x+4)(x^4+16), \quad (x^2+4x+4)(x^4-4x^2+16);$$

  - *$q = 8$ et $f(x)g(x) = (x^2 + 4x + 8)(x^4 - 16x^2 + 64)$;*

- *n est pair et $g(x) = x^4 + \epsilon\sqrt{q}x^3 + qx^2 + \epsilon q\sqrt{q}x + q^2$;*
- *n est impair et fg est l'un des cas suivants*

$$(x^2+q)(x^4+\epsilon\sqrt{2q}x^3+qx^2+\epsilon q\sqrt{2q}x+q^2),$$
$$(x^2\pm\epsilon\sqrt{2q}x+q)(x^4\pm\epsilon\sqrt{2q}x^3+qx^2+\pm\epsilon q\sqrt{2q}x+q^2).$$

– *Les classes d'isogénie de polynôme de Weil h pour $q \neq 4$ contiennent une jacobienne à l'exception des cas suivants :*
- *$q = 2$;*
- *$q = 8$ et $h(x) = (x^2 - 4x + 8)^3$;*
- *$q = 16$ et h est l'un des polynômes suivants :*

$$(x^2+16)^2(x^2-8x+16),\ (x^2+16)(x^2\pm 8x+16)^2,\ (x^2\pm 8x+16)^3,$$
$$(x^2-8x+16)(x^2+8x+16)^2,\ (x^2-4x+16)(x^2\pm 8x+16)^2;$$

- *$q = 64$ et $h(x) = (x^2 - 16x + 64)^3$.*

De plus pour $q = 4$ les classes d'isogénie qui contiennent une jacobienne sont celles pour lesquelles h est divisible par $(x^2 + 2x + 4)(x^2 - 2x + 4)$ ou l'un des polynômes suivants

$$(x^2+4)(x^2\pm 2x+4)^2,\ (x^2+4x+4)(x^2\pm 2x+4)^2,\ (x^2+4)^2(x^2+2x+4),$$
$$(x^2-4x+4)(x^2+4x+4)(x^2-2x+4).$$

Corollaire 2.3.6. *Si $q > 64$ est un carré, il y a toujours une courbe optimale et une courbe minimale de genre 3 sur $\mathbb{F}_q$. Il y a une courbe optimale mais pas de courbe minimale de genre 3 sur $\mathbb{F}_{64}$.*

Remarque 2.3.7. Dans [Oor91a, Prop.5.9], Serre donne ce résultat pour les cas $n = 2n'$ avec n' impair.

Le procédé est constructif. Illustrons cela pour les cas du corollaire 2.3.6. On souhaite ainsi construire des courbes dont les jacobiennes sont isogènes à E_1^3 et à ${E'_1}^3$. On utilise le lemme élémentaire suivant.

Lemme 2.3.8 ([12, Prop.1.4])**.** *Soit $E : y^2 + y = ax^3 + bx^2 + c$ avec $a = u^3$, $u \in k$ et b, tel qu'il existe $v \in k$ avec $va + v^4a^2 = b$. Alors $E \simeq E_1$ si $\mathrm{Tr}_{\mathbb{F}_2}(c + v^3a) = 0$ et $E \simeq E'_1$ sinon.*

Pour E_1^3, prenons $d = e = 0$ dans (2.4) de telle sorte que les courbes elliptiques quotients de (2.5) s'écrivent $E_{\theta_i} : y^2 + y = a_i x^3$ avec $a_i = (g^{-1}\theta_i)^2$. Elles sont isomorphes à E_1 si et seulement si $a_i = x_i^3$ est un cube dans k^*. La somme des racines θ_i devant être nulle, on doit donc trouver $x_1, x_2, x_3 \in k^*$ tel que $x_1^3 + x_2^3 + x_3^3 = 0$. Il est facile de voir que cette équation admet toujours de telles solutions si $q > 16$. Puisque $x_i^3 = (g^{-1}\theta_i)^2$ et $\theta_1\theta_2\theta_3 = g$, on prend $g = (\sqrt[4]{x_1x_2x_3})^{-3}$ et on a également $f = \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3$. Dans un second temps, on conserve les valeurs, de g, f, e et des a_i ci-dessus mais on fait varier d. On cherche $v_i \in k$ tel que

$$\begin{cases} d = v_i + v_i^4 a_i & i = 1,2,3, \\ \mathrm{Tr}_{\mathbb{F}_2}(v_1^3a_1 + v_2^3a_2 + v_3^3a_3) = 1. \end{cases}$$

En effet, par le lemme 2.3.8, cela nous assure que pour les valeurs $b_i = a_i d$, soit une des courbes elliptiques $y^2 = a_i x^3 + b_i x^2$ soit les trois sont isogènes à E_1'.
En posant $a_1 = r^8, a_2 = s^8$ et $a_3 = t^8$, le système d'équations précédent se traduit par l'équation hyperelliptique de genre 4 [12, Lem.5.22]

$$y^2 + y = Ax^9 + Bx^3 \text{ avec } A = (rst)^{-1} \text{ et } B = A(r^7 s + s^7 t + t^7 r)^{1/4}$$

pour laquelle on doit montrer que le nombre de points rationnels est inférieur strictement à $2q + 1$ [12, Lem.4.1]. Pour cela, on utilise des résultats de [vdGvdV92a, Sections 3,5] qui assure que tel est le cas dès que $q > 64$. Il existe donc un $\lambda \in k$ tel que la trace $\mathrm{Tr}_{\mathbb{F}_2}(A\lambda^9 + B\lambda^3) = 1$. Par [12, Lem.4.1], on a les solutions

$$\begin{aligned} v_1 &= (rst)^{-2}(rst\lambda + (r^{-2}t^4 + rs)\lambda^4 + r^{-2}\lambda^{16}), \\ v_2 &= (rst)^{-2}(rst\lambda + (s^{-2}r^4 + st)\lambda^4 + s^{-2}\lambda^{16}), \\ v_3 &= (rst)^{-2}(rst\lambda + (t^{-2}s^4 + tr)\lambda^4 + t^{-2}\lambda^{16}). \end{aligned}$$

On prend $d = v_i + v_i^4 a_i$ pour un i quelconque et on obtient une courbe dont la jacobienne est soit isogène à $E_1'^3$, soit à $E_1 \times E_1 \times E_1'$. Supposons que l'on soit dans le dernier cas. Par dualité, on peut trouver un $e_0 \in k$ tel que [12, Lem.5.1.9]

$$\mathrm{Tr}_{\mathbb{F}_2}(a_1 e_0) = \mathrm{Tr}_{\mathbb{F}_2}(a_2 e_0) = 1 \text{ (et nécessairement } \mathrm{Tr}_{\mathbb{F}_2}(a_3 e_0) = 0).$$

En remplaçant $e = 0$ par $e = e_0$ dans l'équation de la quartique, on obtient ainsi une courbe dont la jacobienne est isogène à $E_1'^3$.

2.4 Courbes de genre 3 avec beaucoup d'involutions sur $\mathbb{F}_{2^n}$

Cette partie se rapporte à l'article [13] avec Enric Nart.

Au vu de la partie 2.3, il était tentant d'appliquer les mêmes idées à d'autres familles de courbes de genre 3.

Définition 2.4.1. Une courbe C de genre 3 sur un corps K a *beaucoup d'involutions* si le groupe des automorphismes de C (sur K) a un sous-groupe de la forme $(\mathbb{Z}/2\mathbb{Z})^2$ et qui ne contient pas l'involution hyperelliptique si C est hyperelliptique.

Comme dans la partie précédente, on peut facilement décomposer à isogénie près la jacobienne de ces courbes de manière explicite en produit de courbes elliptiques. Ceci permet de donner des conditions suffisantes pour "recoller" un triplet de courbes elliptiques et ainsi obtenir des courbes de genre 3 avec de bonnes propriétés arithmétiques. Ces familles sont considérées dans [HLP00] en caractéristique différente de 2 (nous y reviendrons dans la section 4.2.2). Cependant, et contrairement au cas de *loc. cit.*, la conditions de "recollement" est plus simple à exprimer ici. Ceci nous permet d'obtenir l'existence de courbes optimales pour une infinité de $k = \mathbb{F}_{2^n}$ avec n impair.

Par souci d'exhaustivité, nous traitons dans cet article des cas hyperelliptiques et non hyperelliptiques. Il est toutefois évident par des considérations de dimension des

espaces de modules que le recollement de trois courbes elliptiques a une obstruction géométrique dans le cas hyperelliptique (Prop. 2.4.2). Le cas le plus intéressant pour obtenir des courbes optimales est donc le cas non hyperelliptique pour lequel l'obstruction est uniquement de nature arithmétique (Prop. 2.4.3).

2.4.1 Cas hyperelliptique

D'après [NS04, Sec.3], une courbe hyperelliptique de genre 3 a beaucoup d'involutions sur k si et seulement si elle est isomorphe à

$$(\mathrm{Hyp}_a) \qquad C_{a,r,t}: \quad y^2+y = a\left(x+\frac{t}{x}\right)+a(t+1)\left(\frac{1}{x+1}+\frac{t}{x+t}\right)+r,$$

avec a, $t \in k^*$, $t \neq 1$ et $r \in \{0, r_0\}$ ou (exclusif) à

$$(\mathrm{Hyp}_b) \qquad C_{b,r,s,t}: \quad y^2+y = b\left(\frac{1}{x^2+x+s}+\frac{1}{x^2+x+t}\right)+r,$$

avec b, s, $t \in k$, $b \neq 0$, $s, t \notin AS(k)$, $s \neq t$, et $r \in \{0, r_0\}$.

En effectuant le quotient par les involutions, on montre que la jacobienne d'une courbe de la famille (Hyp_a) est isogène à $E_1 \times E_2 \times E_3$ avec

$$\begin{aligned} E_1: \ y^2+xy &= x^3+(r+a(t+1))\,x^2+(a(t+1))^4 \\ E_2: \ y^2+xy &= x^3+(r+a(t+1))\,x^2+(at)^4 \\ E_3: \ y^2+xy &= x^3+(r+a(t+1))\,x^2+a^4. \end{aligned}$$

On obtient un résultat similaire dans le cas de la famille (Hyp_b) avec les courbes

$$\begin{aligned} E_1 \ &: y^2+xy = x^3+r\,x^2+b^4u^{-4}(u+1)^{-4} \\ E_2 \ &: y^2+xy = x^3+(r+r_0)\,x^2+b^4u^4(u+1)^{-4} \\ E_3 \ &: y^2+xy = x^3+(r+r_0)\,x^2+b^4u^{-4}(u+1)^4, \end{aligned}$$

où $u \in k$ est solution de $u(u+1) = s+t$.

Inversement, étant données trois courbes elliptiques E_i/k (ordinaires) de j-invariants j_i, on a le résultat de reconstruction suivant.

Proposition 2.4.2 ([13, Prop.1.4.2])**.** *Il existe une courbe hyperelliptique avec beaucoup d'involutions sur k de quotients elliptiques E_i si et seulement si*

$$\frac{1}{j_1}+\frac{1}{j_2}+\frac{1}{j_3} = 0.$$

2.4.2 Cas non hyperelliptique

On utilise ici les modèles de la partie 2.1. Si on ne tient pas compte du cas supersingulier (abordé dans la partie 2.3), une telle courbe est ordinaire. Ainsi une courbe non

hyperelliptique de genre 3 (ordinaire) a beaucoup d'involutions si et seulement si elle est isomorphe à

$$(\mathrm{NHyp}_a) \qquad C_{a,c,e,r}: \quad (a(x^2+y^2)+cz^2+xy+ez(x+y))^2 = (r(x^2+y^2)+xy)z(x+y+z),$$

avec $a, c, e \in k$, $r \in \{0, r_0\}$, $c \neq 0$ et $a \neq r, r+a+e+c \neq 0$ ou

$$(\mathrm{NHyp}_b) \qquad C_{a,c,d,r}: \quad (a(x^2+y^2)+cz(x+y+z)+dxy)^2 = (r(x^2+y^2)+xy)z(x+y+z),$$

avec $a, c, d \in k$, $r \in \{0, r_0\}$, $cd \neq 0$, $c+d \neq 1$ et $a+dr \neq 0$. Les deux cas ne sont plus mutuellement exclusifs mais ils le deviennent si on ne considère plus seulement des classes d'isomorphisme de la courbe mais de la courbe et d'un couple d'involutions. En effectuant le quotient par les involutions, on montre que la jacobienne d'une courbe de la famille (NHyp_a) est isogène à $E_1 \times E_2 \times E_3$ avec

$$\begin{aligned} E_1 &: y^2+xy &&= x^3+ex^2+(a+r)^2(a+c+e+r)^2 \\ E_2 &: y^2+xy &&= x^3+(e+r)x^2+c^2(a+c+e+r)^2 \\ E_3 &: y^2+xy &&= x^3+(e+r)x^2+c^2(a+r)^2. \end{aligned}$$

Pour la seconde famille, le résultat est similaire avec

$$\begin{aligned} E_1: \quad y^2+xy &= x^3+c^2d^2x^2+d^4(a+dr)^4 \\ E_2: \quad y^2+xy &= x^3+(c^2d^2+r)x^2+c^4(a+dr)^4 \\ E_3: \quad y^2+xy &= x^3+(c^2d^2+r)x^2+(c+d+1)^4(a+dr)^4. \end{aligned}$$

La reconstruction d'une courbe avec beaucoup d'involutions ne fait plus apparaître d'obstruction géométrique mais il y a maintenant une obstruction de nature arithmétique. Celle-ci correspond à l'obstruction de Serre dont nous reparlerons au chapitre 4. Étant donnés $k \neq \mathbb{F}_2$ et une courbe elliptique ordinaire E/k de j-invariant j, on introduit la notation suivante

$$\mathrm{sgn}(E) = \begin{cases} 0, & \text{si } \mathrm{Tr}(E) \equiv 1 \pmod 4, \\ r_0, & \text{si } \mathrm{Tr}(E) \equiv -1 \pmod 4. \end{cases}$$

Ainsi $\mathrm{sgn}(E) = 0$ si et seulement si E a un point de 4-torsion rationnel. La courbe E est isomorphe à $y^2+xy = x^3+\mathrm{sgn}(E)x^2+j^{-1}$. Étant données trois courbes elliptiques ordinaires E_i/k d'invariants j_i on note

$$\mathrm{sgn}(E_1, E_2, E_3) = \mathrm{sgn}(E_1)+\mathrm{sgn}(E_2)+\mathrm{sgn}(E_3) \in \{0, r_0\}.$$

On pose

$$T_a = \frac{(j_1+j_2+j_3)^2}{j_1j_2j_3} \text{ et } \quad T_b = \frac{j_1j_2j_3(j_1+j_2+j_3)}{(j_1j_2+j_1j_3+j_2j_3)^2}.$$

Théorème 2.4.3 ([13, Th.1.4.3]). *Il existe une courbe non hyperelliptique de genre* 3 *(ordinaire) avec beaucoup d'involutions sur k de quotients elliptiques E_i si et seulement si*

$$T_a + \mathrm{sgn}(E_2, E_2, E_3) \in \mathrm{AS}(k) \text{ ou } T_b + \mathrm{sgn}(E_1, E_2, E_3) \in \mathrm{AS}(k).$$

Le premier cas correspond à la famille (NHyp_a) *et le second à la famille* (NHyp_b).

2.4.3 Courbes optimales pour n impair

Supposons que $q > 2$ n'est pas un carré. On a noté $m = \lfloor 2\sqrt{q} \rfloor$.

Théorème 2.4.4 ([13, Th.4.1]). *Si $m \equiv 1, 5, 7 \pmod 8$ il existe une courbe optimale de genre 3 sur $\mathbb{F}_q$.*

Remarque 2.4.5. Pour $m \equiv 0, 2, 6 \pmod 8$, on obtient des courbes C de genre 3 avec un défaut 3 sur $\mathbb{F}_q$, c.-à-d. $\#C(\mathbb{F}_q) = q + 1 + 3m - 3$. Ce sont des courbes maximales si $\{2\sqrt{q}\} < 1 - 4\cos^2(3\pi/7) \approx 0.8019$ (où on a noté $\{a\}$ la partie fractionnaire de a).

Illustrons la méthode de démonstration dans le cas le plus simple, $m \equiv 1 \pmod 4$ et $q \neq 2$. On sait qu'il existe une courbe elliptique ordinaire E avec $q + 1 + m$ points. De plus $\mathrm{sgn}(E) = 1 = \mathrm{sgn}(E, E, E)$ et $T_b = 1$. Ainsi $T_b + \mathrm{sgn}(E, E, E) = 0 \in \mathrm{AS}(k)$ et il existe une courbe C dans la famille (NHyp_b) telle que $\mathrm{Jac}\, C \sim E^3$. En particulier C est optimale. Le procédé est explicite dès que le j-invariant j de E est connu puisque l'on peut prendre

$$C : (j^{-1/4}(x^2 + y^2) + z^2 + xy + xz + yz)^2 = xyz(x + y + z).$$

Un jeu sur les parties entières et fractionnaires de la suite $(2^i\sqrt{2})_{i\in\mathbb{N}}$ permet d'obtenir l'existence d'une courbe optimale de genre 3 pour une infinité de valeurs de q qui ne sont pas des carrés [13, Cor.4.2]. À notre connaissance, il s'agit du premier résultat de ce type pour des courbes de genre strictement supérieur à 2 et des extensions de degré impair d'un corps fini.

Remarque 2.4.6. Si $m \equiv 3 \pmod 8$, il existe encore une courbe elliptique ordinaire $E/\mathbb{F}_{2^n}$ de trace $-m$ et de j-invariant j. En prenant pour j_1, j_2, j_3 des conjugués de j dans le théorème 2.4.3, il est souvent possible de satisfaire à l'une des conditions et d'obtenir ainsi une courbe optimale. Malheureusement, nous ne savons pas démontrer que cette procédure aboutit toujours.

Question : Peut-on démontrer que cette stratégie fonctionne toujours ?

2.5 Projet de recherche

Comme l'illustre ce chapitre, trouver de bons modèles est le point de départ de recherches aussi bien géométriques (calcul des invariants, groupe d'automorphismes) qu'arithmétiques. Leurs résultats servent ensuite de base à des applications en cryptographie (voir le chapitre 5) ou en théorie des codes. On propose ici un projet de recherche sur ces thèmes pour les courbes de genre 3 sur un corps K de caractéristique p quelconque. Certaines questions sont d'un abord assez simples et pourraient constituer ainsi une bonne introduction à la recherche pour un étudiant de Master ou un doctorant. On trouvera dans l'exposé `http://iml.univ-mrs.fr/~ritzenth/slides/expo_ESF.pdf` une présentation de certains de ces problèmes sous forme de transparents.

2.5.1 À propos des modèles

Tout d'abord, qu'entendons nous par "bons modèles", ou plus précisément une famille de bons modèles sur un corps K ? Intuitivement, cette famille doit cerner au plus près les classes d'isomorphismes sur K ou de $\bar{K}$-automorphismes sur K. Par exemple lorsque K est algébriquement clos, on cherche une famille universelle au dessus de M_g (ou d'un lieu particulier), ou de l'espace des modules avec une donnée additionnelle. L'ajout d'une structure permet en effet de rendre les expressions des paramètres de la famille plus petites. Ceci peut être nécessaire car l'expression des paramètres en fonction des invariants absolus, si elle est faisable, n'est pas toujours utilisable.
Lorsque le corps K est quelconque, pour chaque modèle dont le groupe des $\bar{K}$-automorphismes est non trivial, il faut alors déterminer les tordues (ou effectuer de la descente). C'est la ligne directrice des sections 2.5.2 et 2.5.3.

Quels sont les bons modèles connus pour les classes de K-isomorphismes en genre 3 ?

- Dans le cas d'un corps fini de caractéristique 2, on a obtenu dans la partie 2.1 des familles de bons modèles pour le cas non hyperelliptique. Le cas hyperelliptique est traité dans [NS04].
- Si K est un corps algébriquement clos de caractéristique différente de 2 et la courbe hyperelliptique de genre g, on peut considérer les modèles habituels pour ces courbes, c.-à-d. $y^2 = x(x-1)P(x)$ avec $\deg(P) = 2g-1$. Si K est fini, on peut considérer les orbites galoisiennes des abscisses des points de Weierstrass comme dans [NS04] et [MN02, Sec.3.3]. De plus, les méthodes très générales de [LMNX02] et [MN08] sur les orbites de points sous l'action des groupes linéaires permettent d'obtenir directement certaines informations globales (voir [Nar09] pour le nombre de classes d'isomorphismes de courbes hyperelliptiques).

Reste donc le cas des quartiques lisses en caractéristique différente de 2. On a vu que celles-ci requièrent 15 coefficients alors que l'espace des modules est de dimension 6. La rationnalité de M_3 [Kat96] nous indique qu'il doit même exister une famille générique universelle paramétrée par 6 coefficients mais celle-ci n'est pas connue. De plus, il est très probable que l'expression de ses coefficients soient trop volumineuses pour être exploitable. C'est encore une fois les bitangentes qui semblent offrir l'approche la plus prometteuse. Elles sont au nombre de 28. Récemment, [CS03] et [Leh05] ont montré qu'une courbe de genre 3 était uniquement définie par l'ensemble de ses bitangentes car cet ensemble admet une unique structure symplectique. La reconstruction explicite est connue depuis longtemps ([Rie76] et [16]) lorsque le corps est algébriquement clos et très récemment sur un corps quelconque [Guà09]. On peut montrer que l'ensemble des bitangentes est déterminé par un sous-ensemble particulier de 7 bitangentes appelé ensemble d'Aronhold. Il y a 288 tels sous-ensembles. En passant dans le plan dual, un ensemble d'Aronhold peut être vu comme 7 points en position typique (c.-à-d. 3 points ne sont pas alignés et 6 points ne sont pas sur une conique). Lorsque K est algébriquement clos, on peut fixer 4 points par une transformation projective et la courbe ne dépend alors que de 6 paramètres (les coordonnées affines des 3 derniers points). On retrouve le modèle

dit de Riemann [16]. Si K n'est pas algébriquement clos, on pourra essayer de jouer sur les orbites galoisiennes de ces points, comme on l'a fait dans la partie 2.1, afin d'obtenir des modèles pour les classes d'isomorphisme.
Lorsque l'ensemble d'Aronhold est ordonné, il paramétrise en fait les points de $\mathsf{M}_{3,2}^{\mathrm{nh}}$, l'espace des module des courbes non hyperelliptiques de genre 3 avec une structure symplectique de niveau 2 ([GH04, p.309],[DO88, IX]). À titre d'exemple, en utilisant cette description et ses méthodes de comptage, Nart a obtenu le résultat (non-publié)

$$\#\mathsf{M}_{3,2}^{\mathrm{nh}}(\mathbb{F}_q) = q^6 - 35q^5 + 490q^4 - 3485q^3 + 13174q^2 - 24920q + 18375$$

pour $q > 5$.

Pour aller plus loin, même dans le cas de la caractéristique 2, et obtenir des modèles "sur" M_3, il nous semble essentiel de considérer la question des invariants et de la reconstruction à partir de ces derniers.

2.5.2 Invariants, reconstruction et corps de définition

Considérons tout d'abord la question des invariants.

Pour les courbes hyperelliptiques de genre 3 en caractéristique 0, les invariants sont donnés par Shioda [Shi67]. Il est peu probable que ces invariants soient entiers (au sens d'Igusa) et il serait intéressant de trouver un système d'invariants absolus en toute caractéristique, comme en genre 2 (voir section 2.2.1).

Pour les courbes non hyperelliptiques de genre 3, les invariants séparent les orbites et permettent donc à nouveau de classer les quartiques lisses à $\bar{K}$-isomorphisme près. En caractéristique 0, les invariants de Dixmier-Ohno ont été implantés en MAGMA par Girard et Kohel qui les ont utilisés pour caractériser certaines strates pour les points de Weierstrass [GK06]. Comme le remarquent ces auteurs il est également peu probable que ces invariants soient entiers. À ce titre, il serait intéressant de comparer la réduction de ces invariants modulo 2 à ceux que nous obtenons en caractéristique 2 dans [10]. Peut-on, dans ce cas, trouver 6 générateurs explicites de $\bar{\mathbb{F}}_2(\mathsf{M}_3)$?
Pour toutes les applications effectives que nous allons évoquer dans cette section, les invariants de Dixmier-Ohno (ainsi que les nôtres en caractéristique 2) sont trop peu malléables. La section précédente permet d'envisager une autre approche des invariants, en deux étapes successives : la partie $\mathsf{M}_{3,2}$ où l'on regarde l'invariance de 7 points (ordonnés) du plan sous l'action de $\mathrm{PGL}_2(\bar{K})$, puis la partie finie correspondant au revêtement galoisien $\mathsf{M}_{3,2} \to \mathsf{M}_3$ de groupe $\mathrm{Sp}_6(\mathbb{F}_2)$.

Considérons maintenant le problème de la reconstruction d'une courbe à partir de ses invariants absolus.

Rappelons la situation en genre 2. En caractéristique 0, Mestre [Mes91a] a montré qu'une obstruction arithmétique à la reconstruction d'une courbe à partir de ses in-

variants absolus peut exister et que les corps de définition minimaux d'une courbe C pouvaient être une extension quadratique du corps des modules (qui est ici aussi le corps de définition des invariants absolus et le corps résiduel de M_2 en le point C [Sek85]). Il a aussi donné un algorithme pour reconstruire la courbe lorsque la caractéristique du corps est différente de $2, 3$ et 5 et le groupe des automorphismes réduit au groupe engendré par l'involution hyperelliptique ι. La reconstruction dans les cas des groupes d'automorphismes non triviaux en caractéristique $\neq 3, 5$ se trouve intégralement traitée dans les travaux de [SV04] et [CQ05] et [CNP05]. Avec Reynald Lercier, nous avons complété les cas manquants en caractéristique 3 et 5. Le cas le plus délicat fut le cas générique (de groupe d'automorphismes $\langle\iota\rangle$) pour lequel il nous a fallu construire de nouveaux covariants pour remplacer ceux de [Mes91a] qui étaient soit nuls soit liés. Le programme correspondant est disponible dans la version 2.15 de MAGMA (voir aussi `http://iml.univ-mrs.fr/~ritzenth/programming.html`).

En genre 3 hyperelliptique, nous comptons appliquer des idées similaires au cas du genre 2. La possibilité d'utiliser un raisonnement similaire est suggéré dans [Mes91a, Rem.p.321]). Lorsque le groupe des automorphismes n'est pas réduit à $\langle\iota\rangle$, de nombreux cas sont traités de manière plus simple par la théorie des invariants diédraux [GSS05].

Le cas du genre 3 non hyperelliptique générique est quant à lui totalement ouvert : il faudra attendre d'avoir de meilleurs invariants ou d'autres idées pour s'attaquer à ce problème (peut-être l'approche en deux temps suggérée plus haut ?). En attendant, David Kohel, Enric Nart et moi-même avons abordé les cas des groupes d'automorphismes non trivaux sur les mêmes principes que *loc. cit.*. Ce faisant, nous étudions aussi le problème des corps de définition. Certains cas découlent de propriétés générales :

- les corps de définition minimaux sont égaux au corps des modules lorsque le groupe d'automorphismes est réduit à l'identité ou que le corps est fini.
- En caractéristique 0 et pour une courbe C hyperelliptique de genre quelconque, Shaska [Sha03] a montré qu'il n'y a pas d'obstruction si $\mathrm{Aut}(C)/\langle\iota\rangle$ contient au moins deux involutions. Il conjecturait que c'était aussi le cas si $|\mathrm{Aut}(C)| > 2$. Huggins [Hug07] montre que ceci n'est pas le cas pour une infinité de genres mais le cas du genre 3 reste vrai [GSS05].
- Huggins [Hug05] a aussi des résultats partiels dans les cas non hyperelliptiques.

À l'heure actuelle, il ne nous reste qu'un seul cas à traiter, celui où le groupe d'automorphisme est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

2.5.3 Automorphismes et tordues

Étant donnée une courbe C de genre g sur un corps K, nous souhaitons calculer explicitement un ensemble de représentants des classes de K-isomorphismes de ses tordues (voir section 2.1.1 pour la définition des tordues). En genre 2, pour un corps fini, nous avons résolu cette question avec Lercier et implémenté ce calcul en MAGMA. Nous avons utilisé pour cela les nombreux résultats disponibles ([CNP05], [CQ05], [CN07] et [SV04]).

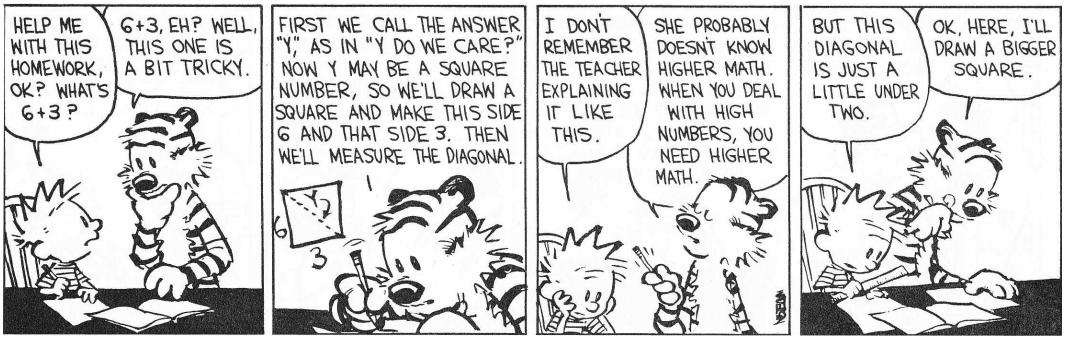
La mise en place d'un programme similaire en genre 3 demande au préalable la connaissance des groupes d'automorphismes sur $\bar{K}$.

- Dans le cas hyperelliptique, [NS04] traite de la caractéristique 2 et [GSS05] la caractéristique 0 (en fait différente de $2, 3$ et 7 par les arguments classiques de [Roq70] et [Gro71, XIII.2.12]). Il est facile de voir qu'en caractéristique 7, il existe une unique exception (la courbe $y^2 = x^7 - x$) dont on connaît le groupe d'automorphismes.
- Dans le cas non hyperelliptique le résultat est connu en caractéristique 2 grâce aux travaux de [Wal95] et en caractéristique 0 (en fait différente de 2 et 3) grâce à ceux de nombreux auteurs : [Hen76], [Ver83], [MSSV02] et [Bar06]. À nouveau, pour la caractéristique 3, une étude devra être entreprise. Remarquons que ce cas n'est pas trivial puisque par exemple la quartique de Klein sur $\bar{\mathbb{F}}_3$ admet comme groupe d'automorphismes le groupe $\mathrm{PSU}_3(\mathbb{F}_9)$ dont l'ordre dépasse la borne de Riemann-Hurwitz. La question est de savoir si cette courbe est la seule exception.

Dans le cas des corps finis, une approche plus algorithmique peut être envisagée et ceci en genre quelconque. Supposons pour simplifier que C est une courbe non hyperelliptique de genre g sur un corps fini K, plongée canoniquement dans $\mathbb{P}^{g-1}$. Soient K'/K une extension de degré m et $\sigma \in \mathrm{Gal}(K'/K)$ l'automorphisme de Frobenius. Soit enfin un K'-automorphisme (nécessairement linéaire) $A \in \mathbf{M}_g(K')$ de C tel que

$$A^{\sigma^{m-1}} \dots A^{\sigma} \dots A = \mathbf{I}_g.$$

La détermination de la tordue de C relativement à A revient alors à chercher une solution à l'équation matricielle $M^{\sigma} = AM$. Ceci peut s'effectuer très efficacement grâce à un algorithme probabiliste [GH97]. Le problème se réduit donc à la détermination rapide de générateurs du groupe des $\bar{K}$-automorphismes pour le plongement canonique. Nous travaillons sur cette question avec Heß.



3 Classes d'isogénie des jacobiennes des courbes de genre 2

Dans ce chapitre, on s'intéresse à la question suivante : étant donnée une classe d'isogénie $\mathcal{A}$ de variétés abéliennes de dimension g sur un corps fini k, $\mathcal{A}$ contient-elle la jacobienne d'une courbe (absolument irréductible, lisse, projective) de genre g ? Depuis Tate, on sait que la classe d'isogénie est déterminée par son polynôme de Weil f. On souhaite donc, plus précisément, une caractérisation de ces classes en termes de propriétés arithmétiques vérifées par les coefficients de f. De tels résultats sont très fructueux : ils permettent en particulier de répondre aux questions sur les courbes maximales (voir Chap. 4) ou sur l'existence de différentes jacobiennes utiles en cryptographie (voir Sec. 5.3.2). Cependant, à notre connaissance, cette question n'est apparue pour la première fois dans la littérature qu'en 1990 dans un article de Rück pour la dimension $g = 2$. Si la dimension $g = 1$ est triviale, puisque toute courbe abélienne est une jacobienne, le genre 2 promettait d'être moins facile : Serre avait trouvé pour une infinité de corps finis des obstructions à l'existence de jacobienne dans certaines classes d'isogénie. Nous allons voir dans ce chapitre que la résolution complète de cette question pour $g = 2$ a pris presque 20 ans et a requis l'utilisation de techniques très diverses. C'est pourquoi, dans la partie 3.1, nous donnons un aperçu des différents arguments qui ont été mis en œuvre dans la résolution du problème. Puis, dans la partie 3.2, nous caractérisons les classes d'isogénie qui contiennent une variété abélienne principalement polarisée, ce qui est une condition nécessaire à l'existence d'une jacobienne. Enfin dans la partie 3.3, nous donnons la solution complète à la question, en étudiant les cas résiduels que sont les cas non-simples et les cas simples supersinguliers.
Les genres 1 et 2 constituent les seuls cas où une réponse complète est connue. On renvoie à la partie 2.3 et au chapitre 4 pour les quelques informations disponibles pour $g = 3$. Signalons, dans une autre direction, une question de Oort tout aussi fascinante, et cependant encore ouverte : toutes les classes de $\bar{k}$-isogénie de variétés abéliennes sur un corps fini k contiennent-elles une jacobienne ?

Notations et conventions pour le chapitre. Soit $\mathcal{A}$ une classe d'isogénie de variétés abéliennes sur k. Par extension, on dit que $\mathcal{A}$ est simple, supersingulière, etc. si un (tous les) élément de $\mathcal{A}$ a cette propriété. On note également $\mathrm{End}^0(\mathcal{A})$ l'algèbre $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ pour un élement $A \in \mathcal{A}$ quelconque. Dans le cas des surfaces

abéliennes, on note $\mathcal{A}_{a,b}$ la classe d'isogénie sur k de polynôme de Weil

$$x^4 + ax^3 + bx^2 + aqx + q^2.$$

Une surface abélienne (ou une classe) sera dite *mixte* si son p-rang est 1.

3.1 Présentation générale des résultats et méthodes

Nous présentons ici les arguments utilisés par différents auteurs pour la résolution de la question en tête de chapitre. Pour faciliter la lecture, nous commençons par décrire les classes d'isogénies en dimension 1 et 2 sur un corps fini.

Remarque 3.1.1. Le mémoire de Master de M. Munsch sous ma direction traite de la description des classes d'isogénie en dimension 3. On consultera également [Xin94] (mais les résultats pour $q = 8, 27$ sont erronés) ainsi que la thèse de Safia Haloui (en préparation sous la direction d'Aubry).

3.1.1 Classes d'isogénie sur un corps fini

La première étape est la détermination des classes d'isogénie des variétés abéliennes sur k. Celle-ci est obtenue en rendant explicites les résultats généraux de la théorie de Honda-Tate (voir [Tat66],[Hon68][Wat69],[WM71],[Tat71]). Dans le cas de la dimension 1, les résultats ont été obtenus par [Wat69] sous la forme suivante : soit t la trace d'une courbe elliptique E sur k.

1. Si $\text{pgcd}(t, p) = 1$ alors E est ordinaire. L'entier t peut prendre toutes les valeurs premières à p dans l'intervalle $-\lfloor 2\sqrt{q} \rfloor \leq t \leq \lfloor 2\sqrt{q} \rfloor$;
2. Si $p|t$ alors E est supersingulière. Les valeurs prises par t sont les suivantes

Condition sur n	Condition sur p	t
n pair	—	$\pm 2\sqrt{q}$
	$p \not\equiv 1 \pmod 3$	$\pm\sqrt{q}$
	$p \not\equiv 1 \pmod 4$	0
n impair	—	0
	$p = 2, 3$	$\pm p^{(n+1)/2}$

Dans le cas de la dimension 2, ceci fut l'objet de plusieurs articles successifs. Lorsque $\mathcal{A}$ est une classe d'isogénie de surfaces abéliennes sur k, [Rüc90] a traité le cas où $\text{End}^0(\mathcal{A})$ est un corps. Puis [Xin96] a considéré les cas supersinguliers en général (mais attention certains cas sont manquants). Enfin [MN02, Lem.2.1,Th.2.9] termine la classification dont voici un résumé.

Théorème 3.1.2. *Le polynôme $f = x^4 + ax^3 + bx^2 + aqx + q^2 \in \mathbb{Z}[x]$ est un polynôme dont les racines sont des nombres de Weil (c.-à-d. un entier algébrique dont la norme pour tout plongement est $\sqrt{q}$) si et seulement si*

$$|a| \leq 4\sqrt{q}, \quad 2|a|\sqrt{q} - 2q \leq b \leq \frac{a^2}{4} + 2q.$$

Table 3.1 – Conditions sur (a, b) pour être une surface abélienne supersingulière.

(a,b)	Conditions sur p	Conditions sur n	L
$(0,0)$	$p \not\equiv 1 \pmod 4$	$\begin{cases} n \text{ pair ou} \\ n \text{ impair et } p \neq 2 \end{cases}$	$\mathbb{F}_{q^2}$
$(0,0)$	$p \equiv 1 \pmod 4$	$\begin{cases} n \text{ pair, } p \not\equiv 1 \pmod 8 \text{ ou} \\ n \text{ impair et } p \neq 2 \end{cases}$	$\mathbb{F}_{q^4}$
$(0,q)$	$p \not\equiv 1 \pmod 3$	n impair	$\mathbb{F}_{q^2}$
$(0,q)$	$p \equiv 1 \pmod 3$	n impair	$\mathbb{F}_{q^6}$
$(0,-q)$	$p \not\equiv 1 \pmod 3$	$\begin{cases} n \text{ pair ou} \\ n \text{ impair et } p \neq 3 \end{cases}$	$\mathbb{F}_{q^2}$
$(0,-q)$	$p \equiv 1 \pmod 3$	$\begin{cases} n \text{ pair, } p \not\equiv 1 \pmod{12} \text{ ou} \\ n \text{ impair et } p \neq 3 \end{cases}$	$\mathbb{F}_{q^3}$
$(\pm\sqrt{q}, q)$	$p \not\equiv 1 \pmod 5$	n pair	$\mathbb{F}_{q^5}$
$(\pm\sqrt{5q}, 3q)$	$p = 5$	n impair	$\mathbb{F}_{q^5}$
$(\pm\sqrt{2q}, q)$	$p = 2$	n impair	$\mathbb{F}_{q^4}$
$(0,-2q)$		n impair	$\mathbb{F}_{q^2}$
$(0,2q)$	$p \equiv 1 \pmod 4$	n pair	$\mathbb{F}_{q^2}$
$(\pm 2\sqrt{q}, 3q)$	$p \equiv 1 \pmod 3$	n pair	$\mathbb{F}_{q^3}$

On note dans ce cas

$$\Delta = a^2 - 4b + 8q, \quad \delta = (a + 2q)^2 - 4qa^2.$$

C'est le polynôme de Weil d'une surface abélienne simple si et seulement si on est dans l'un des trois cas suivants

- Δ *n'est pas un carré dans* $\mathbb{Z}$ *et* $v_p(b) = 0$ *: c'est le cas ordinaire ;*
- Δ *n'est pas un carré dans* $\mathbb{Z}$*,* $v_p(a) = 0$*,* δ *n'est pas un carré dans* $\mathbb{Z}_p$ *et* $v_p(b) \geq n/2$ *: c'est le cas mixte ;*
- (a, b) *appartient au tableau 3.1 : c'est le cas supersingulier. On a noté dans le tableau* L *l'extension minimale sur laquelle* $\mathcal{A}_{a,b}$ *devient non-simple.*

3.1.2 Jacobiennes et surfaces abéliennes

Lorsque q est petit, il est facile de voir que certaines classes d'isogénie ne contiennent pas de jacobienne. Les résultats de Serre sur les courbes maximales en genre 2 ont ensuite indiqué qu'il existe des obstructions à l'existence d'une jacobienne dans certaines classes d'isogénie pour q arbitrairement grand (voir Th. 4.1.1). De nombreuses méthodes ont été conçues pour résoudre le problème en dimension 2 dans sa totalité. Nous avons tenté de les énumérer ci-dessous. Notons que ces méthodes sont parfois appliquées simultanément et en combinaison avec des arguments de descentes et qu'elles peuvent être valables pour

$g \geq 2$.

Nous présentons tout d'abord les méthodes "élémentaires" qui ont souvent l'avantage de donner des résultats constructifs.

1. Grâce à l'ordinateur, pour q petits, on énumère toutes les courbes sur k (ou mieux les classes d'isomorphismes) et on calcule le polynôme de Weil de leur jacobienne. Voir par exemple [MN02, Sec.5]. Ceci peut être rendu optimal en appliquant les méthodes de reconstructions à partir des invariants puis le calcul des tordues, ce que l'on sait faire pour $g = 2$ grâce aux programmes réalisés avec Lercier en MAGMA (version 2.15).
2. Lorsque q est petit, on peut aboutir à des contradictions sur l'hypothèse d'existence d'une courbe en montrant que son nombre de points rationnels serait négatif ou plus petit sur une extension de k que sur k lui-même. Voir par exemple [Rüc90, p.353] et [Lau01, Argument (2.2)].
3. En petites caractéristiques, on peut obtenir une caractérisation pour les classes d'isogénie supersingulières. Pour $p = g = 2$ cela est fait dans [MN07] en utilisant les calculs de fonctions zêta de [vdGvdV92b] et [vdGvdV92a]. On renvoie à la partie 2.3 pour un résultat similaire lorsque $g = 3$. Pour $p = 3$ et $g = 2$, [How08] propose également une solution effective au problème. Pour cela, il montre, entre autres, qu'en caractéristique 3 l'espace des modules grossier des triplets (C, E, ϕ) (C une courbe de genre 2 supersingulière, E une courbe elliptique de j-invariant 0 et $\phi : C \to E$ une application de degré 3) est un revêtement de degré 20 de l'espace des modules grossier des courbes de genre 2 supersingulières.
4. On peut utiliser la structure des automorphismes de la courbe (ou, en combinaison avec le théorème de Torelli (Th.4.1.4), de la variété abélienne principalement polarisée). Ainsi dans [MN02, Appendix], Howe montre que la classe $\mathcal{A}_{0,1-2q}$ ne contient pas de jacobienne. Au contraire, des résultats d'existence peuvent être obtenus pour des familles supersingulières avec beaucoup d'automorphismes en calculant leurs tordues (voir en genre 2 [MN07] qui utilise les familles supersingulières de [IKO86] et la section 4.1.2 en genre 3).

Pour aller plus loin, on utilise le fait qu'une jacobienne est naturellement principalement polarisée. Mieux, le diviseur de cette polarisation est absolument irréductible. Ainsi, si (A, a) est la jacobienne d'une courbe, elle est absolument indécomposable. Rappelons qu'une variété abélienne principalement polarisée (A, a) sur un corps K est *indécomposable* s'il n'existe pas de variétés abéliennes principalement polarisées (A_1, a_1) et (A_2, a_2) sur K telles que $(A, a) \simeq (A_1, a_1) \times (A_2, a_2)$. Inversement, puisque en genre 2 le diviseur de la polarisation a est la courbe dont A est la jacobienne (généralisée), on obtient le résultat suivant.

Théorème 3.1.3 ((Weil) [GGR05, Th.3.1])**.** *Une surface abélienne principalement polarisée sur un corps K est de l'une des formes suivantes*

(a) *la jacobienne d'une courbe de genre 2 sur K ;*
(b) *le produit de deux courbes elliptiques sur K avec la polarisation produit ;*

(c) *la restriction de Weil d'une courbe elliptique définie sur une extension quadratique de K.*

On dit qu'une classe d'isogénie $\mathcal{A}$ est *principalement polarisable* s'il existe une variété abélienne principalement polarisée dans $\mathcal{A}$. Le théorème de Weil nous montre en particulier que si une classe d'isogénie est principalement polarisable et simple sur $\mathbb{F}_{q^2}$ alors c'est la jacobienne d'une courbe. Le contrôle de la polarisation devient alors un facteur déterminant.

5. Rück [Rüc90] utilise des constructions *ad hoc* de diviseurs de polarisations pour montrer que si $\mathcal{A} = \mathcal{A}_{a,b}$ est une classe d'isogénie définie sur $k = \mathbb{F}_p$, telle que $\mathrm{End}^0(\mathcal{A})$ est un corps qui n'est pas une extension galoisienne de $\mathbb{Q}$, et $\mathbb{Z}[(a+\sqrt{d})/2]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, où $d = a^2 - 4b + 8p$, alors $\mathcal{A}$ contient une jacobienne.
6. Howe [How95],[How96] a développé une machinerie très efficace pour déterminer l'obstruction à l'existence d'une polarisation principale dans une classe d'isogénie. Il exprime celle-ci en termes de l'annulation d'un élément d'un groupe construit à partir du groupe de Grothendieck de la catégorie des schémas en groupes finis qui peuvent être plongés dans les éléments de $\mathcal{A}$. On renvoie à la partie 3.2 pour son emploi dans le cas du genre 2.

Lorsque la classe d'isogénie $\mathcal{A}$ est non-simple (ou non-simple sur $\mathbb{F}_{q^2}$) d'autres techniques sont utilisées.

7. Le premier résultat de ce type est la méthode "résultant 1" due à Serre [Lau01, Lem.1] généralisée dans [HL03, Th.1(a)]. Si E_1 et E_2 sont deux courbes elliptiques de trace respective t_1 et t_2 alors la classe d'isogénie de $E_1 \times E_2$ ne contient pas de jacobienne si $|t_1 - t_2| = 1$.
8. Dans le cas où $E^g \in \mathcal{A}$ avec E/k une courbe elliptique ordinaire, Serre a développé une équivalence de catégorie avec les modules hermitiens sur $\mathrm{End}(E)$ (sous de bonnes hypothèses). On renvoie à [Ser85], [Lau02, Appendix] et à la partie 4.4 pour le cas $g = 3$. Dans le cas $g = 2$, en utilisant [Hof91], ceci permet de montrer que lorsque E est de trace t tel que $t^2 - 4q = -3, -4$ ou -7, la classe de $E \times E$ ne contient pas de jacobienne.
9. Dans le cas E^g avec E supersingulière, on peut adapter la théorie précédente en travaillant avec des modules hermitiens quaternioniques. C'est la méthode employée dans la section 3.3.2 combinée avec des arguments de descente.
10. Kani [Kan97] donne des conditions nécessaires et suffisantes pour recoller deux courbes elliptiques le long de leur n-torsion pour $n > 1$. Ceci fut utilisé dans [MV05, Th.8] pour résoudre le cas mixte. On renvoie à la section 3.3.1 pour les détails. Remarquons que dans le cas $n = 2$, les méthodes sont explicites [HLP00, Cor.6] : si E est une courbe elliptique de j-invariant différent de 0 et 1728 et $p > 2$ alors il existe toujours une jacobienne explicite isogène à $E \times E$.
11. Ces arguments peuvent parfois être appliqués globalement. Pour le cas où la classe est simple mais non-simple sur $\mathbb{F}_{q^2}$, on compare le cardinal de l'ensemble des classes

d'isomorphisme de surfaces abéliennes principalement polarisées dans $\mathcal{A}$ au cardinal du sous-ensemble de celles qui sont produits de courbes elliptiques (avec la polarisation produit) sur $\mathbb{F}_{q^2}$. C'est la méthode employée dans [How04] pour montrer qu'il n'existe pas de jacobienne dans la classe $\mathcal{A}_{0,2-2q}$ lorsque $p > 2$. Elle fut ensuite généralisée dans [Mai04] pour les classes $\mathcal{A}_{0,b}$ lorsque $|b| < 2q$, $p \nmid b$ et lorsque $2q - b$ n'est pas un carré dans $\mathbb{Z}$ (c.-à-d. les classes ordinaires, simples mais non-simples sur $\mathbb{F}_{q^2}$). Lorsque $b \neq 1 - 2q$ et $b \neq 2 - 2q$, des bornes sur les nombres de classes montrent qu'il existe toujours une jacobienne dans la classe $\mathcal{A}_{0,b}$. Voir aussi [HN65], [Kan06] pour des résultats semblables dans le cas non-simple.

Nous donnons dans les deux tableaux suivants la solution complète du problème de la caractérisation des classes d'isogénie qui ne contiennent pas de jacobienne pour $g = 2$. Dans la dernière colonne figure l'argument principal qui sert à justifier la condition.

p-rang de $\mathcal{A}$	Conditions sur p et q	Conditions sur s et t	Arguments
—	—	$\lvert s-t\rvert = 1$	(7)
2	—	$s = t$ et $t^2 - 4q \in \{-3, -4, -7\}$	(8)
	$q = 2$	$\lvert s\rvert = \lvert t\rvert = 1$ et $s \neq t$	(1)
1	q carré	$s^2 = 4q$ et $s - t$ sans facteur carré	(10)
0	$p > 3$	$s^2 \neq t^2$	(10)
	$p = 3$ et q qui n'est pas un carré	$s^2 = t^2 = 3q$	(3)
	$p = 3$ et q carré	$s - t$ n'est pas divisible par $3\sqrt{q}$	(3)
	$p = 2$	$s^2 - t^2$ n'est pas divisible par $2q$	(3)
	$q = 2$ ou $q = 3$	$s = t$	(1)
	$q = 4$ ou $q = 9$	$s^2 = t^2 = 4q$	(1)

Table 3.2 – Conditions pour que la classe d'isogénie non-simple $\mathcal{A}$ de polynôme de Weil $(x^2 - sx + q)(x^2 - tx + q)$ ne contienne pas de jacobienne. On suppose ici que $\lvert s\rvert \geq \lvert t\rvert$.

p-rang de $\mathcal{A}$	Condition sur p et q	Conditions sur a et b	Arguments
—	—	$a^2 - b = q$, $b < 0$ et tous les diviseurs premiers de b sont 1 mod 3	(6)
2	—	$a = 0$ et $b = 1 - 2q$	(4)
	$p > 2$	$a = 0$ et $b = 2 - 2q$	(11)
0	$p \equiv 11 \bmod 12$ et q carré	$a = 0$ et $b = -q$	(9)
	$p = 3$ et q carré	$a = 0$ et $b = -q$	(3)
	$p = 2$ et q qui n'est pas un carré	$a = 0$ et $b = -q$	(3)
	$q = 2$ ou $q = 3$	$a = 0$ et $b = -2q$	(1)

Table 3.3 – Conditions pour que la classe d'isogénie simple $\mathcal{A}$ de polynôme de Weil $x^4 + ax^3 + bx^2 + aqx + q^2$ ne contienne pas de jacobienne.

Si $p > 3$, l'ensemble des couples (a, b) tel que la classe d'isogénie de surfaces abéliennes $\mathcal{A}_{a,b}$ contienne une jacobienne, est contenu dans le domaine borné de la figure 3.1.2 auquel il faut retirer un sous-ensemble

- des ronds bleus (resp. noirs) pour lesquels $\mathcal{A}_{a,b}$ est supersingulière (resp. ordinaire) ;
- des courbes noires pour lesquels $\mathcal{A}_{a,b}$ est ordinaire ;
- des points de la courbes vertes pour lesquels $\mathcal{A}_{a,b}$ est mixte.

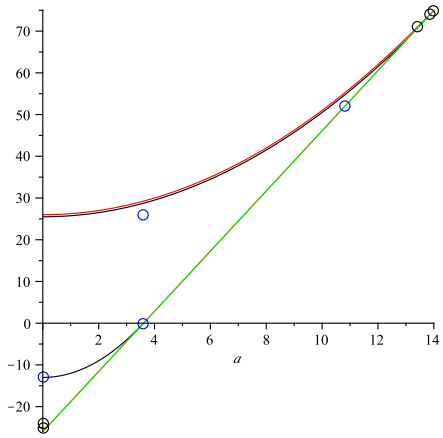


FIGURE 3.1 – Description des couples (a, b) pour les classes d'isogénie de surfaces abéliennes $\mathcal{A}_{a,b}$ qui contiennent une jacobienne sur $\mathbb{F}_q$ avec $p > 3$.

3.2 Existence d'une polarisation principale

Cette partie expose les résultats de [6] avec Everett Howe, Daniel Maisner et Enric Nart.

Le but de l'article est de montrer le résultat suivant.

Théorème 3.2.1 ([6, Th.1])**.** *Soit $\mathcal{A}$ une classe d'isogénie de surfaces abéliennes sur $\mathbb{F}_q$ de polynôme de Weil $f = x^4 + ax^3 + bx^2 + aqx + q^2$. La classe $\mathcal{A}$ n'est pas principalement polarisable si et seulement si les trois conditions suivantes sont satisfaites*

(a) $a^2 - b = q$,
(b) $b < 0$ *et*
(c) *tous les diviseurs premiers de b sont congrus à 1 modulo 3.*

Esquissons la démonstration. Si $\mathcal{A}$ est non-simple, elle est principalement polarisable et il est facile de vérifier qu'une au moins des conditions n'est pas satisfaite. On suppose donc que $\mathcal{A}$ est simple. Soit $\pi \in \mathbb{C}$ une racine de f et $K = \mathbb{Q}(\pi)$. Le corps K est soit totalement réel soit un corps CM, c.-à-d. une extension quadratique imaginaire d'un corps totalement réel K^+. On note $x \mapsto \bar{x}$ la conjugaison complexe. Le problème

de l'existence d'une surface abélienne principalement polarisée dans $\mathcal{A}$ peut être résolu grâce aux techniques développées par Howe. Plus précisément, les résultats d'existence découlent du résultat suivant [How96, Th.1.1].

Théorème 3.2.2. *Si K est totalement réel alors $\mathcal{A}$ est principalement polarisable. Supposons que K est un corps CM. S'il existe un premier fini de K^+ qui se ramifie dans K/K^+ ou un premier de K^+ qui divise $\pi - \bar{\pi}$ et qui est inerte dans K/K^+, alors $\mathcal{A}$ est principalement polarisable.*

Dans le cas ordinaire, grâce à l'équivalence de catégories de [Del69], Howe peut affiner son critère précédent [How95, Cor.11.4]. Cela lui permet de traiter également les cas d'inexistence [How95, Th.13.3]. À sa suite, en utilisant simplement le théorème 3.2.2, [MN02, Th.4.3] démontre le cas mixte sans difficulté car celui-ci est toujours principalement polarisable. Dans l'article, nous franchissons le dernier obstacle en traitant le cas supersingulier.

Soit $\mathcal{A}$ une classe d'isogénie de surfaces abéliennes supersingulières. Si $A \in \mathcal{A}$ n'est pas simple sur $\mathbb{F}_{q^2}$ alors A est isogène à la restriction de Weil d'une courbe elliptique $E/\mathbb{F}_{q^2}$ [6, Lem.4] et donc $\mathcal{A}$ est principalement polarisable. On suppose donc que la classe $\mathcal{A}$ reste simple sur $\mathbb{F}_{q^2}$ (voir [MN02, Tab.1] ou le Th. 3.1.2). Si le polynôme de Weil est réductible alors $[K : \mathbb{Q}] = 2$ et, soit K est totalement réel, soit K est quadratique imaginaire. Le théorème 3.2.2 permet de conclure. Dans les cas restants et à l'exception du cas $\mathcal{A}_{0,-q}$, le théorème s'applique comme le montre le tableau ci-dessous.

(a, b)	Conditions sur p et q	Raison pour la polarisation
$(0, -q)$	$p \equiv 1 \bmod 3$, q n'est pas un carré	—
$(0, -q)$	$p \equiv 7 \bmod 12$, q carré	—
$(0, 0)$	$p \equiv 1 \bmod 4$, q n'est pas un carré	K/K^+ est ramifiée en 2
$(0, 0)$	$p \equiv 5 \bmod 8$, q carré	K/K^+ est ramifié en 2
$(0, q)$	$p \equiv 1 \bmod 3$, q n'est pas un carré	K/K^+ est ramifiée en 3
$(\pm\sqrt{q}, q)$	$p \not\equiv 1 \bmod 5$, q carré	K/K^+ est ramifiée en 5
$(\pm\sqrt{5q}, 3q)$	$p = 5$, q n'est pas un carré	K/K^+ est ramifiée en 5
$(\pm\sqrt{2q}, q)$	$p = 2$, q n'est pas un carré	$\pi - \bar{\pi}$ est divisible par un premier inerte au-dessus de 2

Il reste donc à montrer que la classe $\mathcal{A} = \mathcal{A}_{0,-q}$ n'est pas principalement polarisable lorsque $p \equiv 1 \pmod 3$. Afin de rendre explicites les techniques de Howe décrites dans [6, Th.6], on doit construire une polarisation (non principale) sur une surface abélienne $A \in \mathcal{A}$. Or, on peut montrer que $\mathcal{A}$ contient le noyau A de l'application trace de $\mathrm{Res}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(E) \to E$, où $E/\mathbb{F}_q$ est une courbe elliptique de trace 0 et d'anneau des endomorphismes l'anneau des entiers de $\mathbb{Q}(\sqrt{-q})$ [6, Sec.4]. On construit alors par descente comme dans [How01, Sec.2.2] une polarisation a de degré 9 sur A. On applique finalement le théorème suivant.

Théorème 3.2.3 ([6, Th.6]). *Soit $\mathfrak{A}$ l'idéal de l'anneau des entiers de K^+ tel que le noyau* $\ker(a) = \mathcal{O}/\mathfrak{A}\mathcal{O}$. *Soit ψ l'application d'Artin du groupe des idéaux de l'anneau des entiers de K^+ vers le groupe de Galois de K/K^+ identifié avec $\{\pm 1\}$. La classe d'isogénie $\mathcal{A}$ est principalement polarisable si et seulement si $\psi(\mathfrak{A}) = 1$.*

3.3 Classes d'isogénie et jacobiennes

Cette partie contient les résultats de [7] avec Everett Howe et Enric Nart.

L'article mentionné ci-dessus se scinde en deux parties distinctes : l'étude des classes d'isogénie non-simples et l'étude des classes d'isogénie simples supersingulières qui sont non-simples sur $\mathbb{F}_{q^2}$. Chaque partie se divise en plusieurs sous-cas et nous ne donnerons ici qu'un aperçu des principaux arguments utilisés. Nous invitons le lecteur a se reporter à l'article pour plus de détails.

3.3.1 Cas non-simples

L'idée principale de cette section est d'utiliser les résultats de Kani [Kan97]. Soient E_1 et E_2 deux courbes elliptiques sur k et $m > 0$ un entier. Soit $\psi : E_1[m] \to E_2[m]$ un isomorphisme de schémas en groupes sur k qui est une anti-isométrie par rapport aux couplages de Weil sur $E_1[m]$ et $E_2[m]$. Cette propriété signifie que le diagramme suivant est commutatif

$$\begin{array}{ccc} E_1[m]^2 & \xrightarrow{\psi\times\psi} & E_2[m]^2 \\ \downarrow{\scriptstyle e_1} & & \downarrow{\scriptstyle e_2} \\ \mu_m & \xrightarrow{-1} & \mu_m. \end{array}$$

Soit A la surface abélienne $(E_1 \times E_2)/\mathrm{Graphe}(\psi)$ et $\varphi : E_1 \times E_2 \to A$ l'isogénie correspondante. On a le diagramme commutatif

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{m} & E_1 \times E_2 \\ \downarrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \hat{\varphi}} \\ A & \xrightarrow{a} & \hat{A}. \end{array}$$

On peut montrer [Mil86, Prop.16.8] que le morphisme induit a est une polarisation principale. Inversement, toute polarisation principale sur une surface abélienne non-simple est induite de cette manière pour un certain m. On dira que l'on a "recollé les E_i le long de leur m-torsion". Kani a donné un critère pour que (A, a) soit géométriquement indécomposable. Nous le rappelons ici lorsque m est premier (dans l'article, on utilise aussi le cas $m = 4$).

Théorème 3.3.1 ([Kan97, Th.3]). *Soient m premier, E_1, E_2 et ψ comme ci-dessus. Alors $(E_1 \times E_2)/\mathrm{Graphe}(\psi)$ n'est pas une jacobienne si et seulement s'il existe un entier $0 < i < m$ et une isogénie géométrique $\varphi : E_1 \to E_2$ de degré $i(m-i)$ tel que $i\psi = \varphi|_{E_1[m]}$.*

Soit $\mathcal{A}$ une classe d'isogénie non simple contenant le produit $E_1 \times E_2$ de deux courbes elliptiques sur k. Si la classe n'est pas supersingulière alors soit E_1 est isogène à E_2 sur k, soit isogène après une extension de degré $2, 3, 4, 6$, soit géométriquement non-isogène. Ces cas sont traités successivement par la méthode de Kani et divers arguments de la partie 3.1 [7, Sec.5,6,7]. Par exemple, dans le cas où E_1 et E_2 sont géométriquement non-isogènes, il suffit de produire une anti-isométrie entre les $E_i[m]$. Dans la plupart des cas, $m \neq p$ et $E_i[m]$ est engendré comme module galoisien par un seul élément. Ainsi les modules galoisiens $E_i[m]$ sont isomorphes si et seulement si les traces des deux courbes E_i sont égales modulo m. Si c'est le cas, il existe $\psi : E_1[m] \to E_2[m]$ et $r \in \mathbb{Z}$ tels que le diagramme

$$\begin{array}{ccc} E_1[m]^2 & \xrightarrow{\psi\times\psi} & E_2[m]^2 \\ \downarrow{\scriptstyle e_1} & & \downarrow{\scriptstyle e_2} \\ \mu_m & \xrightarrow{r} & \mu_m \end{array}$$

soit commutatif. En modifiant ψ par $[\ell]$, on modifie r par des carrés modulo m. S'il existe un endomorphisme de E_i d'un degré qui n'est pas un carré modulo m, on peut toujours se ramener au cas $r \equiv -1 \pmod{m}$ et ψ est alors l'anti-isométrie recherchée. L'existence de tels endomorphismes est équivalente à l'existence de premiers totalement décomposés dans $\mathrm{End}^0(E_i)$ qui ne sont pas des carrés modulo m [7, Lem.4.2].

Dans le cas où $\mathcal{A}$ est supersingulière, pour les résultats d'inexistence, on doit également considérer certains schémas en groupes qui ne sont pas étales. On commence par établir la proposition suivante en étudiant les modules de Dieudonné.

Proposition 3.3.2 ([7, Prop.8.1])**.** *Supposons que $p > 3$ et que q est un carré. Soient E_1 et E_2 des courbes elliptiques supersingulières sur $\mathbb{F}_q$ qui ne sont pas isogènes. Alors leurs schémas en groupes $E_1[p]$ et $E_2[p]$ ne sont pas isomorphes.*

Illustrons son utilisation. Notons t_i la trace de la courbe elliptique E_i. Supposons que $t_1 - t_2 = \sqrt{q}$. Alors, si on veut recoller les courbes E_i le long de leur m-torsion pour un certain m, m divise $t_1 - t_2$ donc divise q. Mais les schémas en groupes $E_i[p]$ ne sont pas isomorphes, ceci est donc impossible.

La solution complète dans le cas non-simple est donnée par le tableau 3.2.

3.3.2 Cas simples supersinguliers

On suppose dans toute cette section que $p > 3$ et on note $K = \bar{k}$. L'idée de cette partie est de réaliser des descentes sur des surfaces abéliennes supersingulières principalement polarisées. Ceci se fait en plusieurs étapes :

1. La description géométrique des surfaces abéliennes supersingulières ;
2. La description des polarisations principales sur ces surfaces ;

3. La descente de ces objets. Dans l'article, nous raisonnons en fait sur les tordues. Le point de vue présenté ici est un peu différent et j'espère enrichissant pour le lecteur.

Pour le premier point, on rappelle ci-dessous les résultats de Oort [Oor75]. Soit $E/\mathbb{F}_p$ une courbe elliptique de trace 0. La courbe E est supersingulière et tous ses K-endomorphismes sont définis sur $\mathbb{F}_{p^2}$. Soient $\mathcal{O} = \mathrm{End}_K(E)$ et $\mathcal{B} = \mathcal{O} \otimes \mathbb{Q}$ l'algèbre des quaternions sur $\mathbb{Q}$ de discriminant p. On note $x \mapsto \bar{x}$ l'anti-involution de $\mathcal{B}$. Soit π l'endomorphisme de Frobenius de E sur $\mathbb{F}_p$. On fixe un isomorphisme entre $E[\pi]$ et α_p, où α_p est l'unique schéma en groupe local-local sur $\mathbb{F}_p$. Ainsi, on peut identifier $\mathrm{Hom}_K(\alpha_p, E)$ avec $\mathrm{End}_K(\alpha_p) = K$.
Le noyau de l'application de restriction

$$\begin{aligned} \tilde{}: \mathrm{End}_K(E) &\to \mathrm{End}_K(\alpha_p) \\ u &\mapsto \tilde{u} = u|_{\alpha_p} \end{aligned}$$

est un idéal bilatère $\mathfrak{p}$ de $\mathcal{O}$ au dessus de p, principal (engendré par π), de degré résiduel 2. Cette application induit un plongement naturel de $\mathcal{O}/\mathfrak{p} \hookrightarrow \mathrm{End}_K(\alpha_p) = K$ d'image $\mathbb{F}_{p^2}$. Pour tout couple $(i, j) \in K^2$, on note A_{ij} la surface abélienne sur K donnée par le diagramme suivant

$$0 \to \alpha_p \overset{(i,j)}{\to} E \times E \overset{\psi}{\to} A_{ij} \to 0. \tag{3.1}$$

Il est facile de voir que

$$\begin{aligned} A_{ij} = A_{i'j'} &\iff (i,j)(\alpha_p) = (i',j')(\alpha_p) \\ &\iff \exists a \in K^* \text{ tel que } (i',j') = a(i,j). \end{aligned}$$

Ainsi l'ensemble des A_{ij} (à l'exception de $A_{00} = E \times E$) est paramétré par $\mathbb{P}^1(K)$. Rappelons la définition pour une variété abélienne A/K du *a-nombre*

$$a(A) = \dim \mathrm{Hom}(\alpha_p, A).$$

Pour une surface abélienne supersingulière A, $a(A) \in \{1, 2\}$. On a alors le théorème de classification suivant.

Proposition 3.3.3 ([Oor75, Introduction, Th.2,Cor.7])**.** *Soit A une surface abélienne supersingulière sur K. L'entier $a(A) = 2$ si et seulement si $A \simeq E \times E$. Au contraire, $a(A) = 1$ si et seulement si $A \simeq A_{ij}$ pour $(i : j) \in \mathbb{P}^1(K) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$. De plus si $a(A) = 1$ alors $a(A/\alpha_p) = 2$.*

On appellera le cas $a(A) = 2$ le cas *principal* et $a(A) = 1$ le cas *non-principal*. Comme nous le verrons, ces dénominations proviennent de définitions sur les réseaux quaternioniques hermitiens.

Remarque 3.3.4. On peut également donner une version arithmétique du résultat précédent lorsque $k = \mathbb{F}_{p^n}$ avec n pair. Dans ce cas, si A/k est isogène à E^2 et
– si $a(A) = 2$ alors $A \simeq E^2$;

– si $a(A) = 1$ alors $n > 2$ et il existe $(i : j) \in \mathbb{P}^1(k) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$ tel que $A \simeq A_{ij}$.

Pour le deuxième point (c.-à-d. la description de la polarisation), on procède comme suit [7, Sec.11.3]. Soit a_0 la polarisation produit de $E \times E$. Dans le cas principal, si a est une polarisation principale sur $A = E \times E$, on considère $H = a_0^{-1}a \in \mathrm{End}_K(E \times E) = M_2(\mathcal{O})$. Dans le cas non-principal, si $\psi : E \times E \to A$ est l'isogénie de degré p donnée par le diagramme (3.1) on considère $H = a_0^{-1}\hat{\psi}a\psi \in M_2(\mathcal{O})$. Notons † l'endomorphisme de $M_2(\mathcal{O})$ composé de la transposition et de l'involution sur les coefficients. Cet endomorphisme correspond à l'involution de Rosati sur $\mathrm{End}_K(E^2)$ par rapport à la polarisation produit a_0. Si a_1, a_2 sont deux polarisations principales sur $E \times E$, elles sont isomorphes si et seulement si il existe un isomorphisme $\phi \in \mathrm{Aut}_K(E \times E) = \mathrm{GL}_2(\mathcal{O})$ tel que $a_1 = \hat{\phi}a_2\phi$, c.-à-d.

$$H_1 = a_0^{-1}a_1 = (a_0^{-1}\hat{\phi}a_0)(a_0^{-1}a_2)\phi = \phi^\dagger H_2 \phi.$$

On a ainsi les équivalences suivantes.

Proposition 3.3.5 ([IKO86, Prop.2.8,Prop.2.14])**.** *L'applications $a \mapsto H$ définit une bijection entre l'ensemble des polarisations principales sur A et*

– *dans le cas principal, l'ensemble des matrices*

$$\Lambda^{princ} := \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}),\ st - r\bar{r} = 1 \right\};$$

– *dans le cas non principal, l'ensemble des matrices*

$$\Lambda^{nprinc} := \left\{ \begin{pmatrix} ps & r \\ \bar{r} & pt \end{pmatrix} \in M_2(\mathcal{O}),\ p^2st - r\bar{r} = p \right\}.$$

Dans les deux cas, deux polarisations principales a_1, a_2 sur A sont géométriquement isomorphes si et seulement si leurs matrices H_i sont équivalentes, c.-à-d. il existe $G \in \mathrm{GL}_2(\mathcal{O})$ tel que $H_1 = G^\dagger H_2 G$.

On suppose maintenant, et jusqu'à la fin, que q est un carré. C'est le cas le plus facile car tous les K-endomorphismes et polarisations de $E \times E$ sont rationnels.
Le dernier point est la descente dont nous allons expliquer les grandes lignes. On renvoie à la section 2.1.1 pour des rappels sur la notion de descente. Traitons les cas principaux et non principaux simultanément en associant le symbole $(0 : 0)$ au cas principal. Soit A une surface abélienne supersingulière définie sur $\mathbb{F}_q$. Après une extension de degré l suffisant, on sait que A est $\mathbb{F}_{q^l}$-isogène à $E \times E$. Inversement, on suppose maintenant que A est définie sur $\mathbb{F}_{q^l}$, isogène à E^2, et on étudie les conditions de descente à $\mathbb{F}_q$. Notons $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$ l'automorphisme de Frobenius et $f : A \to A^\sigma$ un $\mathbb{F}_{q^l}$-isomorphisme correspondant à une donnée de descente. D'après la remarque 3.3.4, il existe un couple $(i : j) \in \mathbb{P}^1(\mathbb{F}_{q^l}) \cup \{(0 : 0)\}$ tel que le diagramme suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \alpha_p & \xrightarrow{(i:j)} & E \times E & \xrightarrow{\psi} & A & \longrightarrow & 0 \\ & & \| & & \downarrow \alpha & & \downarrow f & & \\ 0 & \longrightarrow & \alpha_p & \xrightarrow{(i^\sigma:j^\sigma)} & E \times E & \xrightarrow{\psi^\sigma} & A^\sigma & \longrightarrow & 0 \end{array} \tag{3.2}$$

soit commutatif avec $\alpha \in \mathrm{Aut}_K(E\times E) = \mathrm{GL}_2(\mathcal{O})$ induit par f (ψ est un $\mathbb{F}_{q^l}$-isomorphisme dans le cas principal). Ainsi, A descend sur k si et seulement si

$$\alpha^l = 1 \text{ et } \tilde{\alpha}(i:j) = (i^\sigma : j^\sigma)$$

où l'action de $\tilde{\alpha} \in M_2(\mathbb{F}_{p^2})$ sur $\mathbb{P}^1(K)$ est l'action projective usuelle (et $\tilde{\alpha}(0:0) = (0:0)$).

On peut même contrôler la classe d'isogénie de la descente comme suit.

Proposition 3.3.6 ([7, Prop.12.2]). *Soient A et B deux surfaces abéliennes définies sur $\mathbb{F}_q$, d'endomorphisme de Frobenius respectifs π_A et π_B. Soit $\mu : B \to A$ un $\mathbb{F}_{q^l}$-isomorphisme et $h \in \mathbb{Z}[x]$ le polynôme caractéristique de $\alpha = \mu^{-1}\mu^\sigma \in \mathrm{Aut}_{\mathbb{F}_{q^l}}(B)$. Si π_B agit comme un entier sur B alors le polynôme de Weil de A est $\pi_B^4 h(x/\pi_B)$.*

Soit maintenant a une polarisation principale sur $A/\mathbb{F}_{q^l}$. Celle-ci descend pour la donnée f si et seulement si le diagramme suivant commute

$$\begin{array}{ccc} A & \xrightarrow{f} & A^\sigma \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a^\sigma} \\ \hat{A} & \xleftarrow[\hat{f}]{} & \hat{A}^\sigma. \end{array}$$

Avec les notations précédentes, la commutativité du diagramme est équivalente à l'égalité $\alpha^\dagger H \alpha = H$, c.-à-d. α est un automorphismes de la forme quaternionique H (on a utilisé le fait que $H^\sigma = H$ car q est un carré). Les groupes d'automorphismes possibles pour de telles formes sont connus. Leur liste a été établie par Ibukiyama [Ibu89] et Hashimoto et Ibukiyama [HI83] dans le langage des réseaux quaternioniques hermitiens. Ces derniers se répartissent en deux *genres*, appelés *principal* et *non principal*. Après un travail de traduction [7, Sec.11.2], on obtient le résultat suivant dans le cas non principal.

Théorème 3.3.7 ([Ibu89, Th.7.1]). *Soit $p \geq 7$ et notons $\mathrm{Aut}'(H) = \mathrm{Aut}(H)/\{\pm 1\}$ le* groupe réduit des automorphismes *pour $H \in \Lambda^{nprinc}$. Ce groupe est isomorphe à l'un des groupes suivant*

$$\mathbb{Z}/m\mathbb{Z} \text{ pour } m \in \{1,2,3\}, \quad D_{2m} \text{ pour } m \in \{2,3,6\}, \quad A_4, S_4, A_5.$$

De plus le nombre de classes d'équivalence $I(\Gamma')$ de formes hermitiennes de groupe réduit d'automorphismes $\Gamma' = D_{12}, S_4$ ou A_5 est donné par

$$I(D_{12}) = \begin{cases} 1 & \text{si } p \equiv 5 \pmod{12}, \\ 0 & \text{si } p \equiv 1,7,11 \pmod{12}, \end{cases}$$

$$I(S_4) = \begin{cases} 1 & \text{si } p \equiv 3,5 \pmod{8}, \\ 0 & \text{si } p \equiv 1,7 \pmod{8}, \end{cases}$$

$$I(A_5) = \begin{cases} 1 & \text{si } p \equiv 2,3 \pmod{5}, \\ 0 & \text{si } p \equiv 1,4 \pmod{5}. \end{cases}$$

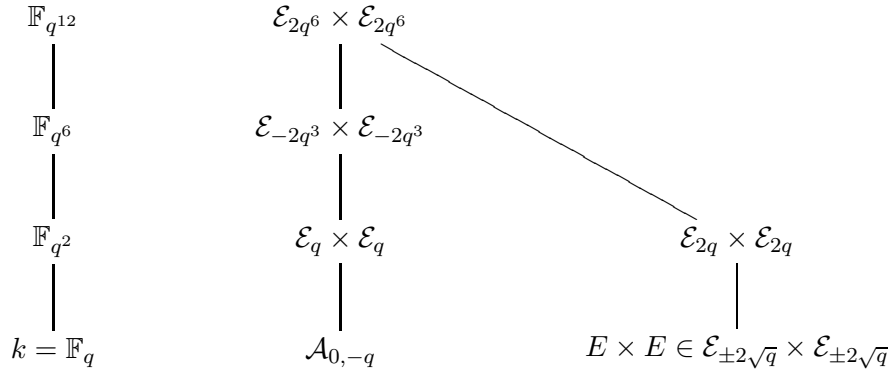
Si $p = 5$, il n'existe qu'une seule forme H (sous l'équivalence précédente) et le groupe réduit des automorphismes est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_5)$.

Remarque 3.3.8. Ce théorème est aussi utilisé dans notre article sous une forme un peu différente. Soient $f \in \mathbb{Z}[x]$ un polynôme unitaire, Γ un sous-groupe de $\mathrm{GL}_2(B)$ et Γ_f l'ensemble des éléments de Γ dont le polynôme caractéristique réduit (en tant qu'élément de $M_2(B)$) est égal à f. Étant donné $f \in \mathbb{Z}[x]$, unitaire de degré 4, on note

$$m(f) = \sum_{i=1}^{h} \frac{\#\Gamma_{i,f}}{\#\Gamma_i},$$

où h est le nombre de classes de $\Lambda^{\mathrm{nprinc}}$ et où les Γ_i sont les groupes d'automorphismes des représentants des classes d'équivalence de $\Lambda^{\mathrm{nprinc}}$. Pour chaque f, Ibukiyama ([Ibu89, Th.2.2] et [HI83, II]) détermine une formule de masse pour les éléments dans Γ_f pour tout Γ et tout f. Ainsi pour $p \geq 7$ et $f = x^4 - x^2 + 1$, $m(f)$ est strictement positive si et seulement si $p \equiv 5 \pmod{12}$. Ceci est en accord avec le cas D_{12} du théorème 3.3.7. En utilisant cette formulation, on dispose aussi de résultats dans le cas principal ([HI83, I.§.5]). Pour le polynôme f ci-dessus on trouve en particulier que la masse est strictement positive si et seulement si $p \equiv 1 \pmod{12}$.

Dans la suite, on note $\mathcal{E}_t$ la classe d'isogénie de courbes elliptiques supersingulières de trace t. Nous souhaitons illustrer l'idée générale pour la classe $\mathcal{A}_{0,-q}$ avec $p \geq 7$ (et q carré). En utilisant les résultats de la partie 3.2, on peut supposer que $p \not\equiv 1 \pmod{3}$, sinon la classe n'est pas principalement polarisable. La classe $\mathcal{A}_{0,-q}$ devient isogène à la classe de $E \times E$ après une extension de degré 12 :



Décrivons tout d'abord les $A \in \mathcal{A}_{0,-q}$. Si $a(A) = 2$, on est dans cas principal et la surface $B = (E \times E)/k$ est une tordue de A. La proposition 3.3.6 nous dit que, si $A \in \mathcal{A}$, alors elle provient de la descente de $E^2/\mathbb{F}_{q^{12}}$ pour la donnée de descente

$$\alpha \in \mathrm{Aut}_K(B) = \mathrm{Aut}(E \times E) = \mathrm{GL}_2(\mathcal{O}), \text{ telle que } \alpha^4 - \alpha^2 + 1 = 0.$$

Si $a(A) = 1$, la condition est similaire pour le K-automorphisme α induit par le diagramme 3.2.
Supposons maintenant que α est un tel automorphisme. Les conditions de descente sont

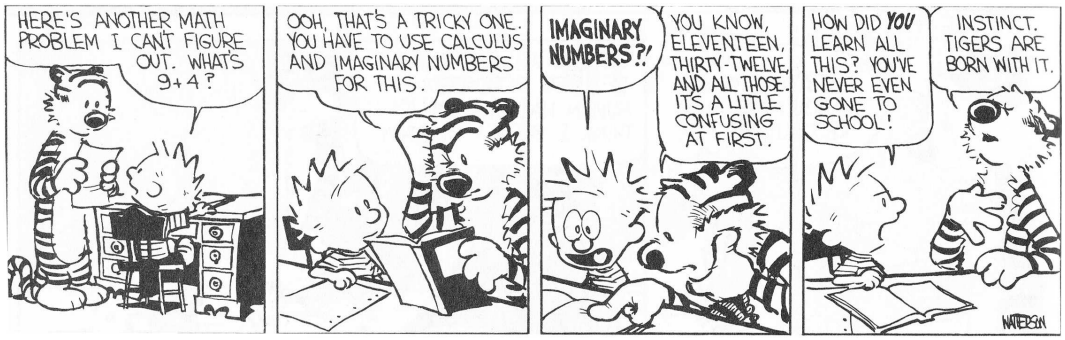
- $\alpha^{12} = 1$ qui est vérifiée ;
- et, dans le cas non-principal, $\tilde{\alpha}(i : j) = (i^\sigma : j^\sigma)$ pour $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^{12}}/\mathbb{F}_q)$ l'automorphisme de Frobenius. Une proposition élémentaire [7, Prop.12.4] montre qu'il existe des éléments de $\mathbb{P}^1(\mathbb{F}_{q^{12}}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$ qui satisfont cette condition.

Il existe donc toujours une surface abélienne $A \in \mathcal{A}_{0,-q}$ avec $a(A) = 1$ et $a(A) = 2$ et toute surface abélienne dans $\mathcal{A}_{0,-q}$ provient des constructions ci-dessus.
On raisonne maintenant sur la polarisation d'une telle A.

- Dans le cas non-principal, le théorème 3.3.7 (ou la remarque 3.3.8) permet de conclure qu'il existe une polarisation principale qui descend sur A si et seulement si $p \equiv 5 \pmod{12}$. Si c'est le cas, comme $a(A) = 1$, cette variété est absolument indécomposable et c'est donc une jacobienne.
- Dans le cas principal, on peut raisonner de même avec la remarque 3.3.8 pour démontrer que A ne peut pas être une jacobienne. On peut également appliquer le raisonnement suivant. Si A était la jacobienne d'une courbe C, alors α serait également un automorphisme de $\mathrm{Jac}\, C$ principalement polarisée et donc de la courbe C. Or, un tel automorphisme satisferait $\alpha^6 = \iota$ et $\alpha^2 \neq \iota$ où ι est l'involution hyperelliptique de C. La classification des groupes d'automorphismes des courbes supersingulières de genre 2 [Igu60, §8] montre qu'il n'existe pas de courbe dont le groupe des automorphismes contient un élément avec ces propriétés.

Remarque 3.3.9. La descente lorsque q n'est pas un carré est un peu plus compliquée car les endomorphismes de E ne sont pas tous rationnels. On renvoie le lecteur à [7, Sec.13.2] pour la manière d'adapter les raisonnements dans ce cas.

La solution complète dans le cas simple supersingulier est donnée par le tableau 3.3.



4 Obstruction de Serre

Pour une courbe sur un corps fini, le nombre de points est certainement la donnée la plus naturelle à étudier. Si l'on fixe la courbe, c'est l'aspect algorithmique qui est prédominant : comment calculer ce nombre rapidement. On peut aussi s'intéresser à des questions globales : par exemple, étant donnée l'ensemble (fini) des courbes (projectives, absolument irréductibles, lisses) de genre $g \geq 0$ sur un corps fini $\mathbb{F}_q$, quel est leur nombre de points minimal, moyen ou maximal ? Cette dernière valeur, notée $N_q(g)$, a été très étudiée, en particulier en raison des applications à la théorie des codes correcteurs d'erreurs. Dans cette optique, on a beaucoup écrit sur les valeurs de $N_q(g)/g$ lorsque g tend vers l'infini avec q fixé. Dans ses cours à Harvard en 1985, Serre traite de cette question mais inverse aussi les rôles et étudie le problème des valeurs de $N_q(g)$ lorsque g est fixé et q varie. Si des résultats sont connus pour certaines valeurs, une formule donnant $N_q(g)$ en général n'est connue que pour $g = 0, 1$ et 2. Dans ce chapitre, nous nous intéresserons au cas du genre 3 pour lequel les résultats ne sont que partiels (les résultats connus pour $g \leq 3$ sont résumés dans la partie 4.1).

Il est assez fascinant de voir que la progression dans les genres est à chaque fois accompagnée de l'apparition d'un aspect totalement nouveau du problème, et pas seulement d'une complexité calculatoire croissante. Ainsi, si l'on peut voir le genre 0 comme un simple exercice de géométrie algébrique, le genre 1 est le premier cas d'application de la théorie de Honda-Tate sur la caractérisation des classes d'isogénie des variétés abéliennes. Avec le genre 2, il devient essentiel de considérer les polarisations et en particulier de montrer l'existence d'une polarisation principale absolument indécomposable. Le chapitre 3 illustre ce principe et répond plus généralement à la question de la caractérisation des classes d'isogénie de surfaces abéliennes qui contiennent une jacobienne. En genre 3 (comme en genre 2 et contrairement au genre 4 ou plus), l'existence d'une telle polarisation est toujours nécessaire et suffisante pour être *géométriquement* une jacobienne. Par contre, contrairement au genre 2, une obstruction à être une jacobienne sur le corps de base apparaît. Elle est observée pour la première fois par Serre qui notait en 1983 : "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée ...)." En 2003, dans une lettre à Top, il formule une stratégie pour déterminer cette mystérieuse racine carrée. Son idée, inspirée par des résultats d'Igusa (Th. 4.2.6) et une formule de Klein (Th. 4.3.10), était qu'il n'y a pas d'obstruction si et seulement si la valeur d'une certaine forme modulaire, notée χ_{18}, est un carré sur le corps. La contribution des papiers résumés dans ce chapitre s'inscrit dans cette stratégie. Dans la partie 4.2, nous validons les assertions de Serre pour une famille de courbes de dimension 3. Cet article nous a permis de formuler clairement le problème

et de déterminer certaines des constantes qui n'étaient pas explicites dans la lettre de Serre. Le second article, présenté dans la partie 4.3, résout le problème en général. Il nous paraît toutefois intéressant de rappeler certains des arguments du premier article car l'approche "basique" qu'on y trouve peut être généralisée et éventuellement donner d'autres formules algébriques intéressantes. La partie 4.4 montre comment déterminer explicitement l'obstruction et en déduire des valeurs de $N_q(3)$.

Malgré ces progrès, on est encore loin d'une formule globale pour $N_q(3)$. On trouvera dans la dernière partie 4.5 quelques pistes pour attaquer cette question délicate. Nous y avons également intégré un projet de recherche algorithmique sur les liens explicites entre la courbe et sa jacobienne car ceci permet d'obtenir des modèles pour les courbes considérées. Certaines des questions qu'on y trouve ne se limitent pas au genre 3.

Notations et conventions pour le chapitre. Lorsque nous parlerons d'une "courbe de genre g", nous sous-entendrons une courbe absolument irréductible, projective et lisse. Étant donné un entier g, on notera $N_q(g)$ le nombre maximum de points d'une courbe de genre g sur $\mathbb{F}_q$. On notera également m l'entier $\lfloor 2\sqrt{q} \rfloor$ et on dira d'une courbe de genre g sur $\mathbb{F}_q$ qu'elle a un *défaut* $a \geq 0$ si son nombre de points est $1 + q + gm - a$. En particulier une courbe de défaut 0 est une courbe optimale (avec la définition de la partie 2.3). On notera aussi $\{x\}$ la partie fractionnaire d'un réel x.

Pour les trois parties concernant les articles, nous avons utilisé les constantes et les notations de l'article le plus récent.

4.1 Courbes maximales en genre $g \leq 3$

Nous rappelons dans cette partie les valeurs ou les meilleures estimations connues de $N_q(g)$ lorsque $g \leq 3$. Pour certaines de ces valeurs et d'autres lorsque $g \leq 50$, nous renvoyons le lecteur à [vdGvdV] ou au site web que nous avons créé avec Gerard van der Geer, Everett Howe et Kristin Lauter : `http://www.manypoints.org`.

4.1.1 Les cas de genre $0, 1, 2$

Le cas $g = 0$

Toute courbe de genre 0 est isomorphe à une conique plane lisse (il suffit d'utiliser le théorème de Riemann-Roch avec l'opposé du diviseur canonique). Sur un corps fini $\mathbb{F}_q$, le théorème de Chevalley-Warning [Ser77, Chap.I.§.2] permet de montrer qu'une conique a un point rationnel. Elle est donc isomorphe à $\mathbb{P}^1$ et $N_q(0) = \#\mathbb{P}^1(\mathbb{F}_q) = q + 1$.

Le cas $g = 1$

Le théorème suivant est un résultat classique dû à Deuring [Deu41] (voir aussi [Wat69]).

Théorème 4.1.1. *L'entier $N_q(1)$ est égal à $q+1+m$ sauf si $n \geq 3$ est impair et p divise m auquel cas $N_q(1) = q + m$.*

Autrement dit sur $\mathbb{F}_{p^n}$, il existe toujours une courbe de genre 1 optimale sauf si $q \neq 2, 3$, n est impair et p divise m auquel cas il n'existe pas de courbe de genre 1 optimale mais une courbe avec un défaut 1.

Le cas $g = 2$

C'est un résultat dû à Serre [Ser83],[Ser85]. On renvoie au chapitre 3 pour le problème plus général des classes d'isogénie qui contiennent une jacobienne.

Théorème 4.1.2. *Si n est pair et $q \neq 4, 9$ alors $N_q(2) = q+1+2m$. De plus $N_4(2) = 10$ et $N_9(2) = 20$. Si n est impair alors $N_q(2) = q+1+2m$ sauf si $p|m$ ou si q peut s'écrire sous la forme x^2+1, x^2+x+1 ou x^2+x+2 avec x entier auxquels cas $N_q(2) = q+2m$ si $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$ et $N_q(2) = q+2m-1$ sinon.*

Ainsi, sauf si $q = 4$, il existe toujours une courbe de genre 2 sur $\mathbb{F}_q$ de défaut $a \leq 2$.

4.1.2 Le cas $g = 3$

Théorème de Torelli arithmétique

Rappelons tout d'abord le résultat d'Oort et Ueno [OU73] en dimension 3.

Théorème 4.1.3. *Soit (A, a) une variété abélienne de dimension 3 principalement polarisée sur un corps K algébriquement clos. Si (A, a) est indécomposable alors (A, a) est la jacobienne d'une courbe de genre 3.*

Le résultat est donc similaire au genre 2 et on pourrait espérer obtenir une formulation arithmétique comme dans le théorème 3.1.3. Néanmoins, la situation n'est pas aussi simple comme le montre le résultat suivant [Lau02].

Théorème 4.1.4. *Soit (A, a) une variété abélienne principalement polarisée de dimension $g \geq 1$ sur un corps K. Supposons que (A, a) soit $\bar{K}$-isomorphe à la jacobienne d'une courbe C_0 de genre g définie sur $\bar{K}$.*

- *Si C_0 est hyperelliptique, il existe une unique courbe C/K de genre g $\bar{K}$-isomorphe à C_0 telle que (A, a) soit isomorphe à $(\mathrm{Jac}\, C, j)$ où j est la polarisation canonique de $\mathrm{Jac}\, C$.*
- *Si C_0 n'est pas hyperelliptique, il existe une unique courbe C/K de genre g $\bar{K}$-isomorphe à C_0 et un unique caractère quadratique*

$$\epsilon : \mathrm{Gal}(K^{sep}/K) \to \{\pm 1\}$$

tels que la variété abélienne tordue par ϵ, notée $(A, a)_\epsilon$, soit isomorphe à $(\mathrm{Jac}\, C, j)$. Le caractère ϵ est trivial si et seulement si (A, a) est isomorphe à la jacobienne d'une courbe de genre g.

La notation $(A, a)_\epsilon$ se comprend comme suit. La variété $(A, a)_\epsilon$ est la tordue quadratique de (A, a) pour le caractère ϵ si, sur une extension au plus quadratique L de K, il

existe un isomorphisme $\phi : (A, a) \to (A, a)_\epsilon$ tel que pour tout $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ on ait l'égalité $(\phi^{-1})^\sigma \circ \phi = \epsilon(\sigma)$. De plus, si $L = K(\sqrt{d})$ où $d \in K/K^2$, alors $\epsilon(\sigma) = \frac{(\sqrt{d})^\sigma}{\sqrt{d}}$. On appellera ainsi, au choix, *obstruction de Serre* la caractère ϵ ou l'entier d.

Remarque 4.1.5. Il est difficile de trouver l'origine exacte de ce résultat. Dans les notes à Harvard [Ser85, 69], Serre indique "Oort +". On trouve effectivement chez Oort (mais en 1991) [Oor91a, Lem.5.7] un théorème proche. Sekiguchi a travaillé sur cette question mais après deux errata, dans [Sek86], il ne donne finalement que l'existence du modèle C/K mais ne parle pas du caractère ϵ. On trouve également mention de ce résultat dans [Maz86, p.236].

Ainsi, dès le genre 3, une courbe pouvant être non hyperelliptique, il peut exister une obstruction à ce que (A, a) définie sur K soit une jacobienne sur K. Cette dichotomie entre le cas hyperelliptique et non hyperelliptique est la conséquence de la théorie de la descente (section 2.1.1) et du théorème de Torelli [Mat58, p.790-792] selon lequel

$$\mathrm{Aut}(\mathrm{Jac}\, C, j) \simeq \begin{cases} \mathrm{Aut}(C) & \text{si } C \text{ est hyperelliptique} \\ \mathrm{Aut}(C) \times \{\pm 1\} & \text{si } C \text{ est non hyperelliptique.} \end{cases}$$

Regardons ce qu'il se passe lorsqu'on cherche à appliquer les techniques du chapitre 3 dans le cas du genre 3. Pour démontrer l'existence d'une courbe avec un nombre de points N sur un corps fini $\mathbb{F}_q$, la plupart des méthodes en genre 2 montrent l'existence d'une "bonne" variété abélienne dans une certaine classe d'isogénie (ici une pour laquelle la trace du Frobenius est $t = 1+q-N$). Supposons cette étape acquise, ce qui en dimension 2 ou 3 revient à démontrer l'existence d'une variété abélienne (A, a) principalement polarisée absolument indécomposable dans cette classe. Alors qu'en dimension 2, cela permet de conclure directement à l'existence d'une courbe de genre 2 avec N points, un tel résultat n'est plus vrai en dimension 3, car il se peut que ce soit la tordue quadratique de (A, a) qui soit une jacobienne et alors le nombre de point sur la courbe serait $(1+q+t)$. En particulier, si l'on cherche à construire une courbe avec beaucoup de points (c.-à-d. avec $t \ll 0$), on peut obtenir une courbe avec très peu de points. Ceci explique la valeur absolue dans le résultat suivant.

Théorème 4.1.6 ([Lau02, Th.3])**.** *Quel que soit le corps fini $\mathbb{F}_q$, il existe une courbe de genre 3 sur $\mathbb{F}_q$ telle que*

$$|\#C(\mathbb{F}_q) - q - 1| \geq 3m - 3.$$

Ce théorème est établi au moyen de raffinements de la méthode (8) de la section 3.1 (voir aussi la partie 4.4). Nous allons le préciser un peu dans les paragraphes suivants.

Les résultats négatifs

Tout comme en genre 2, les arguments du chapitre 3 peuvent toutefois montrer que certaines courbes ne peuvent exister. Ainsi

1. Il n'existe pas de courbe de genre 3 optimale si q est de la forme suivante
   (a) $x^2 + r$ avec x entier, $r = 1$ ou 2 et $r \leq x$;

(b) $x^2 + x + r$ avec x entier, $r = 1$ ou 3 et $r \leq x$.

Ces résultats [Lau02, Th.1,2] proviennent de l'inexistence de certaines formes hermitiennes pour les discriminants $-4, -8, -3$ et -11 (dans l'ordre des r ci-dessus).

2. Il n'existe pas de courbe de genre 3 avec un défaut 1. Ceci est une simple application de l'argument (7) de la partie 3.1.
3. Il n'existe pas de courbe de genre 3 avec un défaut 2 si q est de la forme $x^2 + x + r$ avec $r = 1$ ou 3 et $r \leq x$.

Les résultats partiels

Pour passer outre l'obstruction de Serre et se rapprocher un instant des résultats en genre 2, on définit le *défaut relatif* $a \geq 0$ d'une courbe C de genre 3 comme l'entier a tel que $|\#C(\mathbb{F}_q) - q - 1| = 3m - a$. Si a est le plus petit entier pour lequel il existe une courbe $C/\mathbb{F}_q$ de genre 3 telle que $|\#C(\mathbb{F}_q) - q - 1| = 3m - a$, on appelle a le *défaut relatif minimal*. En particulier $N_q(3) \leq 1 + q + 3m - a$. Avec ces définitions, on peut préciser le théorème 4.1.6 sous la forme suivante [Lau02, Th.1,2,3].

1. si $q = x^2 + r$ avec x entier, $r = 1$ ou 2 et $r \leq x$ alors le défaut relatif minimal est 2 ;
2. si $q = x^2 + x + r$ avec x entier, $r = 1$ ou 3 et $r \leq x$ alors le défaut relatif minimal est 3 ;
3. Dans les autres cas, si m est premier à p alors le défaut relatif minimal est 0. Si $p|m$, il existe une courbe $C/\mathbb{F}_q$ de genre 3 telle que $|\#C(\mathbb{F}_q) - q - 1| = 3m - 3$.

La situation est claire sauf dans le troisième cas lorsque $p|m$. Pouvons nous préciser la situation dans ce cas ?

Rappelons tout d'abord la structure de la jacobienne des courbes de genre 3 de défaut relatif $a \leq 2$ [Lau01]. Lorsqu'une courbe C de genre 3 est de défaut relatif 0, sa jacobienne est isogène à E^3, où E est une courbe elliptique de trace $\pm m$. En effet, on peut montrer (voir la démonstration de [13, Cor.4.2]) qu'il n'existe pas de variété abélienne simple sur $\mathbb{F}_q$ de polynôme de Weil $(x^2 \pm mx + q)^3$. Le défaut relatif 1 est impossible comme on l'a vu. Soit

$$\chi_C = \prod_{i=1}^{3}(x - \alpha_i)(x - \bar{\alpha}_i) = \prod_{i=1}^{3}(x^2 + s_i x + q)$$

le polynôme de Weil de la jacobienne d'une courbe C de genre 3 avec un défaut relatif 2. En utilisant [Lau01, Tab.1] et [HL03, Th.1] on a les possibilités suivantes pour les valeurs des s_i :

Cas	s_i	Condition
1	$\pm m, \pm m, \pm(m-2)$	—
2	$\pm m, \pm(m+\sqrt{3}-1), \pm(m-\sqrt{3}-1)$	$\{2\sqrt{q}\} \geq \sqrt{3}-1$
3	$\pm(m+1-4\cos^2\frac{\pi}{7}), \pm(m+1-4\cos^2\frac{2\pi}{7}), \pm(m+1-4\cos^2\frac{3\pi}{7})$	$\{2\sqrt{q}\} \geq 1-4\cos^2\frac{3\pi}{7}$

Si n est pair, il existe une courbe elliptique supersingulière E de trace $\pm m$. Le résultat [Ibu93, Th.3] donnant l'existence d'une polarisation principale absolument indécomposable sur E^3 lorsque p est impair, le défaut relatif minimal est 0. Lorsque $p = 2$, le théorème 2.3.5 montre que le défaut relatif minimal est aussi zéro sauf si $q = 4$ ou $q = 16$, cas pour lesquels le défaut relatif minimal est 3.
Si n est impair, le tableau des traces de courbes elliptiques de la section 3.1.1 montre qu'il n'existe pas de courbe supersingulière de trace $\pm m$ sauf si $q = 2$ ou 3. Puisque $2 = 1^2 + 1$, le défaut relatif minimal est 2 (mieux, il existe une courbe de genre 3 sur $\mathbb{F}_2$ de défaut 2). De même puisque $3 = 1^2 + 1 + 1$, le défaut relatif minimal est 3 (mieux, il existe une courbe de genre 3 sur $\mathbb{F}_3$ de défaut 3). Supposons donc $q > 3$. Il n'existe alors pas de courbe de genre 3 de défaut relatif 0 ou qui appartienne au cas 1 ou 2 du tableau ci-dessus. Le cas 3 correspond à une variété abélienne absolument simple (et même ordinaire ici) et [How96, Th.1.2] montre que cette classe est principalement polarisable. Ainsi si $\{2\sqrt{q}\} \geq 1 - 4\cos^2\frac{3\pi}{7}$, le défaut relatif minimal est 2, sinon il est égal à 3. On obtient ainsi l'analogue du théorème 4.1.2, à l'obstruction près.

Proposition 4.1.7. *Si n est pair et $q \neq 4, 16$ alors le défaut relatif minimal est 0. Si $q = 4$ ou 16, il est égal à 3. Si n est impair, le défaut relatif minimal est 0 sauf si*

- *$q = x^2 + r$ avec x entier, $r = 1$ ou 2 et $r \leq x$ pour lequel le défaut relatif minimal est 2 ;*
- *ou si $q = x^2 + x + r$ avec x entier, $r = 1$ ou 3 et $r \leq x$ pour lequel le défaut relatif minimal est 3 ;*
- *ou si $p \mid m$ pour lequel le défaut relatif minimal est 3, sauf si $\{2\sqrt{q}\} \geq 1 - 4\cos^2\frac{3\pi}{7}$ pour lequel il est égal à 2.*

Remarque 4.1.8. Rybakov [Ryb08] a obtenu une "quasi-caractérisation" de l'existence d'une polarisation principale absolument indécomposable dans le cas d'un produit $B \times E$ d'une surface abélienne absolument simple B et d'une courbe elliptique ordinaire E. Ses résultats n'étant pas encore publiés nous les rappelons ici et en tirons une conséquence élémentaire.
Soit $\chi_B = x^4 + ax^3 + bx^2 + qax + q^2$ et $\chi_E = x^2 - tx + q$ les polynômes de Weil respectifs de B et E. Soit K^+ l'extension quadratique réelle de $\mathbb{Q}$ définie par $P = x^2 + ax + b - 2q$ et $K = End^0(E)$. On note δ et Δ les discriminants respectifs de K^+ et K.

Définition 4.1.9. On dit qu'un premier $\ell \neq p$ et 2 est *exceptionnel* si

- ℓ divise $P(t)$;
- χ_E est irréductible modulo ℓ ;
- ℓ^2 divise $a^2 - 4b + 8q$;
- ℓ ne divise pas δ.

Le premier 2 est exceptionnel si

- t est impair ;
- 4 divise $a + b + 1 - 2q$;
- 2 ne divise pas δ.

On a alors le théorème suivant.

Théorème 4.1.10. *S'il existe dans la classe d'isogénie de $B \times E$ une variété abélienne principalement polarisée et absolument indécomposable, alors une des conditions suivantes est réalisée :*

1. *Il existe un premier ℓ non-exceptionnel qui divise $P(t)$;*
2. *Il existe des premiers exceptionnels $\ell_1, \ldots, \ell_m$, des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, des entiers naturels $\alpha_1, \ldots, \alpha_m$ tels que $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_m^{\alpha_m}$ est un idéal premier de K^+ engendré par un élément totalement positif et $\ell^{\alpha_i} | P(t)$ pour tout i ;*
3. *p divise $P(t)$.*

Inversement, il existe dans la classe d'isogénie de $B \times E$ une variété abélienne avec une polarisation absolument indécomposable si l'une des conditions (2)*,* (3) *ou* (4) *est satisfaite avec* (4) *la condition suivante*

4. *Il existe un premier non exceptionnel ℓ divisant $P(t)$ et*
   - *si $\chi_E \equiv (x-\alpha)^2 \pmod{\ell}$ alors $\ell^2 | \chi_E(\alpha)$;*
   - *si $\Delta = -\ell$ et $\ell \equiv 3 \pmod 4$ alors $\chi_E \not\equiv (x-\alpha)^2 \pmod{\ell}$ pour tout α.*

Si $p \neq 2, 3$, $p \nmid m$ et si $\{2\sqrt{q}\} \geq \sqrt{3} - 1$, le critère [HZ02] montre que le cas 2 correspond au produit d'une courbe elliptique ordinaire et d'une surface abélienne ordinaire absolument simple. Des calculs élémentaires montrent alors qu'il existe dans la classe d'isogénie de $B \times E$ une variété abélienne principalement polarisée et absolument indécomposable.

Les résultats positifs

Pour les petites valeurs de q, on renvoie à [Top03] ainsi qu'à `www.manypoints.org` qui complète ces résultats et corrige les modèles de courbes pour $p = 41$ et $p = 47$.
Commençons par les cas n pairs pour lesquels nos connaissances sont plus complètes.

- Si $p = 2$, le corollaire 2.3.6 montre qu'il existe une courbe optimale de genre 3 sur $\mathbb{F}_{2^n}$ si $n \geq 6$. De plus $N_4(3) = 1+q+3m-3 = 14$ et $N_{16}(3) = 1+q+3m-3 = 38$.
- Si $p \equiv 3 \pmod 4$, on sait [Ibu93, p.2] qu'il existe une courbe optimale de genre 3. Cette courbe est hyperelliptique d'après les résultats de [Oor91a] mais n'est pas explicite (voir toutefois [KTW09] pour des sous-cas explicites). De plus, la courbe de Fermat $x^4 + y^4 + z^4 = 0$ est optimale si $n \equiv 2 \pmod 4$.
- Pour $p \equiv 1 \pmod 4$ et $n \equiv 2 \pmod 4$, Ibukiyama *(loc. cit.)* démontrer qu'il existe aussi une courbe optimale. Dans tous les cas, la stratégie d'Ibukiyama est d'utiliser les formules de masses sur les formes hermitiennes quaternioniques afin de démontrer l'existence d'une variété abélienne principalement polarisée et absolumenent indécomposable dans une certaine classe sur $\mathbb{F}_p$. La variété et sa tordue quadratique étant isomorphes sur $\mathbb{F}_{p^2}$, il évite ainsi la question de l'obstruction de Serre.

Passons au cas n impair pour lequel la situation est plus fragmentaire.

– Si $p = 2$, on utilise les résultats de la section 2.4.4. Si $m \equiv 1, 5, 7 \pmod 8$, il existe une courbe optimale de genre 3 sur $\mathbb{F}_{2^n}$. Si $m \equiv 0, 2, 6 \pmod 8$, il existe une courbe de genre 3 et de défaut 3 sur $\mathbb{F}_{2^n}$, maximale si $\{2\sqrt{q}\} < 1 - 4\cos^2(3\pi/7)$.

– Si $p = 3$, [AT02] montre qu'il existe une courbe C de genre 3 sur $\mathbb{F}_{3^n}$ avec un défaut inférieur à 21. Pour cela, les auteurs utilisent la famille de quartiques

$$x^4 + y^4 + z^4 = (\lambda + 1)(x^2y^2 + y^2z^2 + z^2x^2).$$

Comme remarqué par les auteurs, en utilisant [HLP00] (voir la section 4.2.2) et la famille plus générale des quartiques de Ciani, on obtient un défaut inférieur à 9. Tout récemment, Mestre [Mes] a utilisé une nouvelle famille, avec groupe d'automorphismes S_3, et obtient un défaut inférieur à 3. De plus, si $n \geq 7$ et $3 \nmid m$ alors il existe une courbe optimale sur $\mathbb{F}_{3^n}$.

– Si $p = 7$, Mestre dans *loc. cit.* montre qu'il existe une courbe C de genre 3 sur $\mathbb{F}_{7^n}$ avec un défaut inférieur à 9. De plus, si $3|m$ et $-m$ est un carré non nul modulo 7, alors il existe une courbe optimale sur $\mathbb{F}_{7^n}$.

– La stratégie de Serre mise en place dans [7'] (voir la partie 4.4) permet de vérifier l'existence de certaines courbes optimales lorsque $m^2 - 4q = -7, -19, -43, -67$ ou -163 (voir aussi [AAMZ09] pour une approche plus directe dans le cas -19). On obtient par exemple l'existence d'une courbe optimale de genre 3 pour les valeurs $q = 47, 61, 137, 277$ et 23^3.

Remarquons que toutes ces méthodes utilisent des familles de courbes avec beaucoup d'automorphismes et dont la jacobienne est isogène à un produit de courbes elliptiques. Toutefois, afin d'obtenir des résultats systématiques, on n'exploite pas complètement les conditions algébriques obtenues. En caractéristique 2, par exemple, la remarque 2.4.6 indique qu'on peut espérer couvrir d'autres cas. De même, pour un corps K de caractéristique différente de 2, dans le cas le plus simple de la section 4.2.2, c.-à-d. $E_1 = E_2 = E_3 : y^2 = x(x - \alpha)(x - \beta)$ avec $\alpha, \beta \in K$, il existe une jacobienne isogène à E_1^3 si $3\alpha + \beta \in K^2$. Ainsi, pour un q donné, si les résultats de la partie ne donnent pas immédiatement la réponse, on peut souvent tenter de vérifier à la main si l'une des conditions est remplie. Mestre [Mes] a ainsi obtenu des courbes optimales, dans la famille qu'il considère, sur $\mathbb{F}_p$ pour $p < 10000$ dans 90% des cas.

4.2 Obstruction de Serre pour les quartiques de Ciani

Cette partie expose les résultats de l'article [8] obtenus avec Gilles Lachaud.

Pour une famille de dimension 3 de quartiques lisses (les quartiques de Ciani), l'article [HLP00] avait trouvé une formulation algébrique de l'obstruction de Serre. En utilisant les formules de duplication et de transformation des ThetaNullwerte (théorèmes 4.2.2 et 4.2.1), nous avons établi le lien entre cette condition et la forme modulaire $\widetilde{\chi}_{18}$ (voir Th. 4.2.14). Ceci nous a permis de préciser la formule de l'obstruction selon Serre [8, Letter to Top]. Nous commencerons par rappeler dans cette partie les éléments de théorie complexe des variétés abéliennes dont nous aurons besoin dans les trois parties suivantes. Puis nous donnerons notre formulation des résultats de [HLP00] et pour terminer des

éléments de la démonstration que nous avons suivie.

Notations et conventions pour la partie. L'entier g est supérieur à 1.

4.2.1 Variétés abéliennes sur $\mathbb{C}$ et formes modulaires

La référence pour cette partie est le livre [BL04].

Variétés abéliennes

On note

$$\mathbf{J}_g = \begin{bmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{bmatrix}$$

où $\mathbf{1}_g$ est la matrice unité de taille g. Soit la matrice $\Omega \in \mathbf{M}_{g,2g}(\mathbb{C})$, où les vecteurs colonnes forment une base de $\mathbb{C}^g$ sur $\mathbb{R}$. Cette matrice engendre un réseau $\Lambda = \Omega\mathbb{Z}^{2g}$. Soit $\mathcal{R}_g$ l'ensemble des matrices $\Omega \in \mathbf{M}_{g,2g}(\mathbb{C})$ satisfaisant aux *conditions de Riemann*

$$\Omega.\mathbf{J}_g.{}^t\Omega = 0 \quad \text{et } 2i(\bar{\Omega}.\mathbf{J}_g^{-1}.{}^t\Omega)^{-1} > 0$$

(> 0 signifiant définie positive). On appelle une telle matrice une *matrice des périodes*. Si $\Omega \in \mathcal{R}_g$ alors le tore $A_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^{2g}$ est une variété abélienne de dimension g munie d'une polarisation principale j dont la première classe de Chern est représentée par la forme hermitienne $H = 2i(\bar{\Omega}\mathbf{J}_g^{-1}{}^t\Omega)^{-1}$ [BL04, Lem.4.2.3].

Inversement, soit (A, a) une variété abélienne principalement polarisée définie sur $K \subset \mathbb{C}$. La *matrice des périodes* de (A, a) définie par les bases $\omega_1, \ldots, \omega_g$ du K-espace vectoriel $H^0(A, \Omega^1_A \otimes K)$ et une base symplectique $\gamma_1, \ldots, \gamma_{2g}$ de $H_1(A, \mathbb{Z})$ pour la polarisation a, est la matrice

$$\Omega = \begin{pmatrix} \int_{\gamma_1} \omega_1 & \cdots & \int_{\gamma_{2g}} \omega_1 \\ \vdots & & \vdots \\ \int_{\gamma_1} \omega_g & \cdots & \int_{\gamma_{2g}} \omega_g \end{pmatrix}.$$

On a $\Omega \in \mathcal{R}_g$ et (A, a) est $\mathbb{C}$-isomorphe à (A_Ω, j).

Le groupe $\mathrm{GL}_g(\mathbb{C})$ agit sur $\mathcal{R}_g$ à gauche par changement de base de $\mathbb{C}^g$. Si on écrit

$$\Omega = [\Omega_1\ \Omega_2], \quad \text{où } \Omega_i \in \mathbf{M}_g(\mathbb{C}),$$

on a $W.[\Omega_1\ \Omega_2] = [W.\Omega_1\ W.\Omega_2]$ pour $W \in \mathrm{GL}_g(\mathbb{C})$. Cette action induit un isomorphisme entre les variétés abéliennes. En particulier, si on choisit $W = \Omega_2^{-1}$ alors A_Ω est isomorphe à $A_\tau = \mathbb{C}^g/[\tau\ \mathbf{1}_g]\mathbb{Z}^{2g}$ avec $\tau = \boldsymbol{\tau}(\Omega) = \Omega_2^{-1}\Omega_1$. Avec ces notations, un matrice complexe $\Omega \in \mathbf{M}_{g,2g}(\mathbb{C})$ appartient à $\mathcal{R}_g$ si et seulement si $\boldsymbol{\tau}(\Omega) \in \mathbb{H}_g$ où $\mathbb{H}_g$ est le demi-plan de Siegel défini par

$$\mathbb{H}_g = \{\tau \in \mathbf{M}_g(\mathbb{C}),\ {}^t\tau = \tau,\ \mathrm{Im}\,\tau > 0\}.$$

On dit que τ est une *matrice de Riemann*. Le groupe symplectique $\Gamma_g = \mathrm{Sp}_{2g}(\mathbb{Z})$ agit sur $\mathcal{R}_g$ à droite par changement de base symplectique du réseau Λ. Si $\Omega \in \mathcal{R}_g$ et $M \in \Gamma_g$,

$$\Omega.M = [\Omega_1,\ \Omega_2] \begin{bmatrix} A & B \\ C & D \end{bmatrix} = [\Omega_1 A + \Omega_2 C\ \Omega_1 B + \Omega_2 D].$$

Cette définition induit une action sur le demi-plan de Siegel : si $\tau \in \mathbb{H}_g$, on note

$$M.\tau = (A\tau + B)(C\tau + D)^{-1}.$$

Les deux actions sont liées par $M.\boldsymbol{\tau}(\Omega) = \boldsymbol{\tau}(\Omega.{}^tM)$.

Fonctions thêta et formes modulaires

Pour une approche plus moderne de la théorie des caractéristique thêta, on renvoie à [GH04]. On appelle *caractéristique thêta* $[\boldsymbol{\varepsilon}] = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix}$ un élément de $\mathbb{Z}^g \oplus \mathbb{Z}^g$. Une caractéristique est *paire* (resp. *impaire*) si $\varepsilon_1 \cdot \varepsilon_2 \equiv 0 \pmod 2$ (resp. $\varepsilon_1 \cdot \varepsilon_2 \equiv 1 \pmod 2$). Soit S_g l'ensemble des caractéristiques thêta paires à coefficients 0 ou 1. Le cardinal de S_g est égal à $2^{g-1}(2^g + 1)$. On fait agir $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Gamma_g$ par

$$[M.\boldsymbol{\varepsilon}] = \begin{bmatrix} D\varepsilon_1 - C\varepsilon_2 + (C^tD)_0 \\ -B\varepsilon_1 + A\varepsilon_2 + (A^tB)_0 \end{bmatrix}$$

où P_0 est une notation pour le vecteur diagonal d'une matrice carrée P.

Pour $\tau \in \mathbb{H}_g$ et $[\boldsymbol{\varepsilon}]$ une caractéristique thêta, on définit la *fonction thêta* (de caractéristique $[\boldsymbol{\varepsilon}]$) de variable $z \in \mathbb{C}^g$ par la série convergente

$$\theta \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} (z, \tau) = \sum_{n \in \mathbb{Z}^g} \exp\left(i\pi(n + \varepsilon_1/2)\tau^t(n + \varepsilon_1/2) + 2i\pi(n + \varepsilon_1/2) \cdot (z + \varepsilon_2/2) \right).$$

On appelle *ThetaNullwert* la valeur en $z = 0$ de cette fonction et on écrit

$$\theta[\boldsymbol{\varepsilon}](\tau) = \theta \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} (\tau) = \theta \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} (0, \tau).$$

La fonction thêta de caractéristique $[\boldsymbol{\varepsilon}]$ étant paire (resp. impaire) si sa caractéristique est paire (resp. impaire), les ThetaNullwerte sont nulles si $[\boldsymbol{\varepsilon}]$ est impaire. Ainsi, dans la suite, lorsqu'on parle d'une ThetaNullwert, on supposera que la caractéristique de celle-ci est paire.

Ces fonctions peuvent être vues comme certaines sections de fibrés sur la variété abélienne A_τ. Elles satisfont les deux formules ci-dessous qui traduisent respectivement l'action d'un changement de base symplectique et le pull-back par l'isogénie $A_{\tau/2} \to A_\tau$.

Proposition 4.2.1 (Formule de transformation [Igu72, V.§.2]). *Pour $M \in \Gamma_g$*

$$\theta[M.\boldsymbol{\varepsilon}](M.\tau) = \kappa(M) \cdot \exp\left(\frac{i\pi}{4} \cdot \phi_{[\varepsilon_1,\varepsilon_2]}(M)\right) \cdot j(M,\tau)^{1/2} \cdot \theta[\boldsymbol{\varepsilon}](\tau) \tag{4.1}$$

où $\kappa(M)^2$ est une racine de l'unité ne dépendant que de M,

$$j(M,\tau) = \det(C\tau + D)$$

et

$$\phi_{[\varepsilon_1,\varepsilon_2]}(M) = \varepsilon_1 {}^tDB{}^t\varepsilon_1 - 2\varepsilon_1 {}^tBC{}^t\varepsilon_2 + \varepsilon_2 {}^tCA{}^t\varepsilon_2 - 2(D\varepsilon_1 - C\varepsilon_2)^t(A^tB)_0.$$

Proposition 4.2.2 (Formule de duplication [RF74, Cor.IIA2.1], [Igu72, IV.th.2]). *Soient $\begin{bmatrix}\varepsilon_1\\ \varepsilon_2\end{bmatrix}$ et $\begin{bmatrix}\varepsilon_1\\ \delta\end{bmatrix}$ deux caractéristiques thêta et $\tau \in \mathbb{H}_g$. Alors*

$$\theta\begin{bmatrix}\varepsilon_1\\ \varepsilon_2\end{bmatrix}(\tau/2) \cdot \theta\begin{bmatrix}\varepsilon_1\\ \delta\end{bmatrix}(\tau/2) = \sum_{\mu \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\mu\delta} \cdot \theta\begin{bmatrix}\varepsilon_1 - \mu\\ \varepsilon_2 - \delta\end{bmatrix}(\tau) \cdot \theta\begin{bmatrix}\mu\\ \varepsilon_2 - \delta\end{bmatrix}(\tau). \tag{4.2}$$

On introduit maintenant les formes modulaires de Siegel analytiques (classiques selon la terminologie de [vdG08]).

Définition 4.2.3. On appelle *forme modulaire (de Siegel analytique) de poids h et de genre g* (pour le groupe Γ_g), une fonction holomorphe $f : \mathbb{H}_g \to \mathbb{C}$ telle que pour tout $\tau \in \mathbb{H}_g$ et tout $M \in \Gamma_g$ on ait

$$f(M.\tau) = j(M,\tau)^h f(\tau).$$

De plus lorsque $g = 1$, on demande que f soit holomorphe en $i\infty$.

On note $\mathbf{R}_{g,h}(\mathbb{C})$ l'espace vectoriel des formes modulaires de Siegel analytiques de poids h et de genre g.

Les ThetaNullwerte ne sont pas des formes modulaires au sens ci-dessus (ce sont des formes modulaires de poids $1/2$ pour le sous-groupe de congruence $\Gamma_g(4,8)$ de Γ_g) mais elles forment les briques élémentaires pour en construire, en utilisant des polynômes symétriques pour le quotient $\Gamma_g/\Gamma_g(4,8)$. Dans la suite, nous aurons besoin des formes modulaires suivantes. Soient $g \geq 2$ et $h = \#S_g/2 = 2^{g-2}(2^g+1)$, on note

$$\widetilde{\chi}_h(\tau) = \frac{(-1)^{gh/2}}{2^{2^{g-1}(2^g-1)}} \cdot \prod_{\boldsymbol{\varepsilon} \in S_g} \theta[\boldsymbol{\varepsilon}](\tau).$$

Igusa [Igu67, Lem.10] a montré que pour $g \geq 3$, le produit $\widetilde{\chi}_h$ est une forme modulaire analytique de poids h pour Γ_g.

Remarque 4.2.4. L'utilité de la constante que nous introduisons dans la définition de $\widetilde{\chi}_h$ apparaîtra plus tard.

Lorsque $g = 2$, $\widetilde{\chi}_{10}$ n'est qu'une formule modulaire pour un sous-groupe de congruence mais son carré est une forme modulaire pour Γ_2.

Pour $g = 3$, nous aurons également besoin de la forme modulaire $\tilde{\Sigma}_{140} \in \mathbf{R}_{3,140}(\mathbb{C})$ qui est la fonction symétrique élémentaire de degré 35 en les puissances huitième des ThetaNullwerte.

Relation avec la jacobienne

Soit C une courbe de genre g sur un corps $K \subset \mathbb{C}$. Classiquement, $(\operatorname{Jac} C)(\mathbb{C})$ est un tore $\mathbb{C}^g/\Lambda$ que l'on peut décrire comme $H^0(C, \Omega^1_C \otimes K)^*/H_1(C, \mathbb{Z})$ où à $\gamma \in H_1(C, \mathbb{Z})$, on associe la forme linéaire $\eta \mapsto \int_\gamma \eta$. Plus spécifiquement, si $\gamma_1, \ldots, \gamma_{2g}$ est une base de $H_1(C, \mathbb{Z})$ pour le couplage d'intersection sur C et $\eta_1, \ldots, \eta_g$ une base de $H^0(C, \Omega^1)$ alors

$$\Omega = \begin{pmatrix} \int_{\gamma_1} \eta_1 & \cdots & \int_{\gamma_{2g}} \eta_1 \\ \vdots & & \vdots \\ \int_{\gamma_1} \eta_g & \cdots & \int_{\gamma_{2g}} \eta_g \end{pmatrix}$$

est une matrice des périodes pour $\operatorname{Jac} C$.

Les relations entre la courbe et sa jacobienne sont extrêmement riches. Les ThetaNullwerte donnant les coefficients d'un plongement de la jacobienne dans $\mathbb{P}^{4^g-1}$ sont des données fondamentales et il est donc important de savoir comment les obtenir en fonction des coefficients de la courbe. Dans le cas hyperelliptique, il s'agit des formules de Thomae (voir [Mum07], [Guà02, Th.11.1]). Inversement, la reconstruction de la courbe à partir de sa jacobienne (polarisée) est théoriquement possible d'après le théorème de Torelli. En genre 2 et 3 hyperelliptique, on a les formules dites de Rosenhain (voir [Wen03] et [Wen01]). Pour le cas du genre 3 non hyperelliptique, nous renvoyons le lecteur à la section 4.5.3.

Formes modulaires en dimension $g \leq 3$

Notons $\mathbf{R}_g = \oplus_h \mathbf{R}_{g,h}(\mathbb{C})$. La structure de ces $\mathbb{C}$-algèbres sont connues pour les petites valeurs de g. Pour $g \leq 3$, celle-ci est bien sûr très fortement connectée à la structure des algèbres d'invariants classiques (voir la section 2.2.1).

En genre 1, l'algèbre $\mathbf{R}_1$ est engendrée par les deux séries d'Eisenstein de poids respectifs 4 et 6

$$\widetilde{g}_2(\tau) = 60 \cdot \sum_{a,b \in \mathbb{Z}\setminus\{0,0\}} (a\tau + b)^{-4} \quad \text{et } \widetilde{g}_3(\tau) = 140 \cdot \sum_{a,b \in \mathbb{Z}\setminus\{0,0\}} (a\tau + b)^{-4}.$$

En genre 2, la structure et les générateurs de $\mathbf{R}_2$ proviennent de résultats d'Igusa [Igu62] et [Igu64] (on renvoie aussi à [vdG08, p.200] pour des références plus complètes et une démonstration). Enfin, en genre 3, Tsuyumine, [Tsu86] donne 34 générateurs explicites construits à partir des ThetaNullwerte.

On connaît l'interprétation géométrique de certaines de ces formes modulaires. Par exemple, en genre 1, notons $\widetilde{\Delta}(\tau) = \widetilde{g}_2^3 - 27\widetilde{g}_3^2$. C'est une forme modulaire (cuspidale) de poids 12 qui admet l'expression suivante en fonctions des ThetaNullwerte

$$\widetilde{\Delta} = \frac{1}{2^8} \cdot \left(\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \theta \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right)^8 \in \mathbf{R}_{1,12}(\mathbb{C}).$$

Soit $E : y^2 = f(x)$ avec f un polynôme unitaire de degré 3, une courbe elliptique sur $\mathbb{C}$ de matrice des périodes $[\Omega_1\ \Omega_2]$ pour la forme différentielle $dx/(2y)$ et une base symplectique de $H_1(E, \mathbb{Z})$. Soit δ le discriminant de f, comme défini dans la section 2.2.1 (c'est $-1/16$ fois le discriminant de E de [Sil92, p.50]). Alors [Loc94, Prop.3.2]

$$\delta = -\frac{(2i\pi)^{12}}{2^{16}} \cdot \frac{\widetilde{\Delta}(\boldsymbol{\tau}(\Omega))}{\Omega_2^{12}}.$$

En genre 2, on a un résultat similaire [Gra88, Prop.2.5]. Soit $C : y^2 = f(x)$ une courbe de genre 2 sur $\mathbb{C}$ avec $f \in \mathbb{C}[x]$ de degré 5 unitaire. Soit $\Omega = [\Omega_1\ \Omega_2]$ une matrice des périodes de $\operatorname{Jac} C$ pour une base symplectique quelconque de $H_1(C, \mathbb{Z})$ et la base de différentielles régulières $dx/(2y), xdx/(2y)$. Le discriminant δ de f est lié à la forme $\widetilde{\chi}_{10}^2$ par la formule

$$\delta = \frac{(2i\pi)^{20}}{2^{28}} \cdot \frac{\widetilde{\chi}_{10}^2(\boldsymbol{\tau}(\Omega))}{\det(\Omega_2)^{10}}.$$

De plus, $\widetilde{\chi}_{10}(\tau) = 0$ si et seulement si (A_τ, j) est décomposable.

Remarque 4.2.5. Il y a plus généralement une relation entre un certain produit de $\binom{2g+1}{g}$ puissances huitièmes de ThetaNullwerte et le discriminant des courbes hyperelliptiques [Loc94, Prop.3.2,3.3]. C'est une conséquence des formules de Thomae.

En genre 3, Igusa [Igu67, Lem.10,11] a montré le joli résultat suivant.

Théorème 4.2.6. *Si $\tau \in \mathbb{H}_3$, alors :*

1. *(A_τ, j) est décomposable si et seulement si $\widetilde{\chi}_{18}(\tau) = \widetilde{\Sigma}_{140}(\tau) = 0$.*
2. *(A_τ, j) est la jacobienne d'une courbe hyperelliptique de genre 3 si et seulement si $\widetilde{\chi}_{18}(\tau) = 0$ et $\widetilde{\Sigma}_{140}(\tau) \neq 0$.*
3. *(A_τ, j) est la jacobienne d'une courbe non hyperelliptique de genre 3 si et seulement si $\widetilde{\chi}_{18}(\tau) \neq 0$.*

Klein [Kle90, Eq.118,P.462] a donné une relation entre la forme $\widetilde{\chi}_{18}$ et le discriminant des quartiques planes comme défini dans la section 2.2.1. Nous donnons dans [3'] une démonstration de cette formule avec la constante précise (voir Th. 4.3.10).

Remarque 4.2.7. En genre 3, il existe aussi une interprétation par les invariants irrationnels [Giz07].

4.2.2 Quartiques de Ciani et les résultats de [HLP00]

Dans cette section, K désigne un corps de caractéristique différente de 2.

Quartiques de Ciani

Ciani [Cia99] a donné en 1899 une classification des quartiques non singulières, basée sur le nombre d'involutions dans le groupe des automorphismes. Pour

$$s = \begin{bmatrix} a_1 & b_3 & b_2 \\ b_3 & a_2 & b_1 \\ b_2 & b_1 & a_3 \end{bmatrix} \in \mathbf{Sym}_3(K),$$

on définit une *quartique de Ciani* C_s par le polynôme

$$Q_s(x,y,z) = a_1x^4 + a_2y^4 + a_3z^4 + 2(b_1y^2z^2 + b_2x^2z^2 + b_3x^2y^2).$$

Cette quartique n'est pas nécessairement lisse mais son groupe d'automorphismes a un sous-groupe de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ engendré par

$$\sigma_1(x,y,z) = (-x,y,z) \text{ et } \sigma_2(x,y,z) = (x,-y,z).$$

Lorsque la quartique est lisse c'est donc une courbe avec beaucoup d'involutions selon la définition 2.4.1. Inversement,

Proposition 4.2.8 ([8, Prop.2.1])**.** *Si C est une quartique plane lisse définie sur un corps K (de caractéristique différente de 2) avec beaucoup d'involutions, alors il existe une matrice $s \in \mathrm{Sym}_3(K)$ telle que C soit isomorphe à C_s.*

La démonstration donnée dans l'article est incomplète. Nous en donnons une nouvelle version ci-dessous.

Démonstration. Soient M_1, M_2 les matrices dans $\mathrm{GL}_3(K)$ de deux involutions non triviales qui commutent. On a $M_i^2 = \lambda_i \mathbf{I}_3$ avec $\lambda_i \in K$. Puisque $\det(M_i)^2 = \lambda_i^3$, chaque λ_i est un carré dans K et on peut supposer que $M_i^2 = \mathbf{I}_3$. De plus $M_1M_2 = \lambda M_2M_1$. En appliquant le déterminant, on a de nouveau $\lambda^3 = 1$. Si $\lambda = 1$, les matrices M_i commutent et donc se diagonalisent dans la même base. Après un changement de coordonnées, on peut supposer que M_1 et M_2 sont projectivement équivalentes à

$$S_1 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ et } S_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Ceci montre qu'une équation de la quartique C dans ces coordonnées n'a que des monômes de degré pair et c'est donc une quartique de Ciani.
Il reste à montrer que $\lambda = 1$. Soit P une matrice telle que $P^{-1}M_1P = S_1$ par exemple. On peut écrire

$$(P^{-1}M_1P)(P^{-1}M_2P) = S_1(P^{-1}M_2P) = \lambda(P^{-1}M_2P)(P^{-1}M_1P) = \lambda(P^{-1}M_2P)S_1.$$

Comme S_1 agit par multiplication par -1 sur la première ligne ou sur la première colonne, l'égalité précedente force λ à être égal à ± 1. Mais -1 est impossible car $\lambda^3 = 1$. □ □

Remarque 4.2.9. Le cas de la caractéristique 2 est étudié à la section 2.4.2.

Nous souhaitons maintenant caractériser les matrices s pour lesquelles C_s est lisse. L'exemple 2.2.4 nous donne une formule pour le discriminant de ces courbes.

Proposition 4.2.10 ([8, Prop.2.2])**.** *Soit $s \in \mathrm{Sym}_3(K)$ et $c_i = a_ja_k - b_i^2$ le cofacteur de a_i pour $1 \leq i \leq 3$. Alors*

$$\mathrm{Disc}\, Q_s = 2^{40}a_1a_2a_3(c_1c_2c_3)^2 \det(s)^4.$$

On note $\mathbf{S}$ l'ensemble des matrices symétriques telles que $a_i \neq 0$ et $c_i \neq 0$ pour $1 \leq i \leq 3$ et $\mathbf{S}^\times = \mathbf{S} \cap \mathrm{GL}_3(K)$. La quartique C_s est lisse si et seulement si $s \in \mathbf{S}^\times$.

Les résultats de [HLP00]

La présentation matricielle ci-dessus nous permet de jeter un nouvel éclairage sur les résultats de [HLP00, Sec.4]. Soient

$$E_i : y^2 = x(x^2 - 4b_i x - 4c_i), \quad b_i \in K, c_i \in K^*,$$

trois courbes elliptiques et soit $\delta_i = b_i^2 + c_i$. On suppose qu'il existe une racine carrée $\rho \in K^*$ de $\delta = \delta_1\delta_2\delta_3$ et on note $\tilde{\mathbf{A}}$ l'ensemble des couples constitués d'un tel produit $A = E_1 \times E_2 \times E_3$ et de ρ. À un élément $(A, \rho) \in \tilde{\mathbf{A}}$ on associe une matrice

$$s(A,\rho) = \begin{bmatrix} a_1 & b_3 & b_2 \\ b_3 & a_2 & b_1 \\ b_2 & b_1 & a_3 \end{bmatrix} \in \mathsf{S}, \quad a_i = \rho/\delta_i.$$

Inversement à $s \in \mathsf{S}$, on associe l'élément de $(A(s), \rho(s)) \in \tilde{\mathbf{A}}$ défini par

$$E_i : y^2 = x(x^2 - 4b_i x - 4c_i), \quad c_i = a_j a_k - b_i^2, \qquad (i = 1, 2, 3)$$

et $\rho(s) = a_1a_2a_3$. Le lemme [8, Lem.2.2] montre que ces applications sont des bijections réciproques.
Suivant [HLP00, Lem.13], on considère sur un triplet $A = E_1 \times E_2 \times E_3$ comme ci-dessus un sous-groupe isotrope maximal indécomposable et rationnel W de $A[2]$ (il y en a 54). En étiquetant les points de $E_i[2](\bar{K})$ par

$$Q_i = (0,0), \quad P_i = (2b_i + \rho_i, 0), \quad R_i = (2b_i - \rho_i, 0),$$

on peut écrire W sous la forme

$$W = \left\{ \begin{array}{cccc} (O,O,O), & (O,Q_2,Q_3), & (Q_1,O,Q_3), & (Q_1,Q_2,O), \\ (P_1,P_2,P_3), & (P_1,R_2,R_3), & (R_1,P_2,R_3), & (R_1,R_2,P_3) \end{array} \right\}.$$

L'application qui à (A, W) fait correspondre $(A, \rho_1\rho_2\rho_3) \in \tilde{\mathbf{A}}$ est une bijection [8, Lem.2.3]. Ainsi, à $s \in \mathbf{S}$, on associe successivement $(A(s), \rho(s))$ puis $(A(s), W_{\rho(s)})$. Notons enfin $A'(s)$ la variété abélienne principalement polarisée telle que $A'(s) = A(s)/W_{\rho(s)}$, la polarisation principale étant induite par deux fois la polarisation produit sur $A(s)$. La proposition suivante est une reformulation de [HLP00, Prop.15].

Théorème 4.2.11 ([8, Th.2.1,2.2])**.** *Pour tout $s \in \mathbf{S}^\times$ notons $Cof(s) \in \mathbf{S}^\times$ la matrice des cofacteurs de s. Alors $(\operatorname{Jac} C_s, j)$ est isomorphe à $A'(Cof(s))$.*
Inversement, $A'(s)$ est isomorphe à la jacobienne d'une courbe (non hyperelliptique) si et seulement si $\det s$ est un carré dans K^*.

La deuxième partie du théorème représente donc l'obstruction de Serre. Elle se déduit aisément de la première partie et du lemme élémentaire suivant.

Lemme 4.2.12. *L'application $s \mapsto Cof(s)$ induit une suite exacte*

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}_3(K) \xrightarrow{Cof} G^{\times 2}(K) \longrightarrow 1$$

avec

$$G^{\times 2}(K) = \{s \in \mathrm{GL}_3(K),\ \det s \in K^{*2}\}.$$

Remarque 4.2.13. L'obstruction de Serre est donc égale à $\det s$. Dans [HLP00], elle est égale à $T = 64 \det s$.
Dans le cas où $s \in \mathbf{S} \setminus \mathbf{S}^{\times}$, on a $\det(s) = 0$ et $A'(s)$ est la jacobienne d'une courbe hyperelliptique [HLP00, Prop.14].

4.2.3 Interprétation analytique

Le dernier objectif de l'article était de comparer l'obstruction algébrique $\det s$ et $\widetilde{\chi}_{18}$ sur $A'(s)$. On suppose dans cette section que $K \subset \mathbb{C}$.

Une expression liée à $\det s$

Soit $s \in \mathbf{S}$ et

$$X(s) = 2^{80}(a_1\, a_2\, a_3)^4\, (c_1\, c_2\, c_3)^2\ \det s = 2^{80}\delta^2\, (c_1\, c_2\, c_3)^2\ \det s.$$

Cette quantité est un carré si et seulement si $\det s$ est un carré. De plus, on a la relation

$$X(\mathrm{Cof}(s)) = \mathrm{Disc}(C_s)^2$$

qui, en prévision de la formule de Klein (Th. 4.3.10), semble être la bonne quantité à considérer. En intégrant la forme différentielle $dx/(2y)$ (et non pas dx/y comme dans l'article), on a l'uniformisation suivante pour les $E_i : y^2 = x(x^2 - 4b_i x - 4c_i)$

$$E(w_{1i}, w_{2i}) : y^2 = x\left(x - \frac{(2i\pi)^2}{w_{2i}^2}\theta\begin{bmatrix}0\\0\end{bmatrix}(\tau_i)^4\right)\left(x - \frac{(2i\pi)^2}{w_{2i}^2}\theta\begin{bmatrix}0\\1\end{bmatrix}(\tau_i)^4\right),$$

avec $[w_{1i}, w_{2i}] \in \mathcal{R}_1$ et $\tau_i = \frac{w_{1i}}{w_{2i}} \in \mathbb{H}_1$. Après calculs des b_i, c_i et δ_i en ces termes, on obtient [8, p.302]

$$X(s) = -2^{40} \cdot (2i\pi)^{54} \cdot (w_{21}w_{22}w_{23})^{-18} \cdot \left(\prod_{i=1}^{3} \theta_{0i}^8 \theta_{2i}^8 (\theta_{0i}^4 - \theta_{2i}^4)^3\right) \cdot \mathsf{R}_1$$

où on a posé

$$\theta_{0i} = \theta\begin{bmatrix}0\\0\end{bmatrix}(\tau_i), \quad \theta_{1i} = \theta\begin{bmatrix}1\\0\end{bmatrix}(\tau_i), \quad \theta_{2i} = \theta\begin{bmatrix}0\\1\end{bmatrix}(\tau_i),$$

$$\mathsf{a} = \theta_{01}^2\theta_{02}^2\theta_{23}^2, \quad \mathsf{b} = \theta_{01}^2\theta_{22}^2\theta_{03}^2, \quad \mathsf{c} = \theta_{21}^2\theta_{02}^2\theta_{03}^2, \quad \mathsf{d} = \theta_{21}^2\theta_{22}^2\theta_{23}^2$$

et

$$\mathsf{R}_1 = (\mathsf{a}+\mathsf{b}+\mathsf{c}+\mathsf{d})(\mathsf{a}+\mathsf{b}-\mathsf{c}-\mathsf{d})(\mathsf{a}-\mathsf{b}-\mathsf{c}+\mathsf{d})(\mathsf{a}-\mathsf{b}+\mathsf{c}-\mathsf{d}).$$

L'expression de $\widetilde{\chi}_{18}$ sur $A'(s)$

Soit $s \in \mathbf{S}$, nous souhaitons exprimer $\widetilde{\chi}_{18}$ sur $A'(s)$. Pour cela il nous faut

1. expliciter une matrice des périodes Ω' de $A'(s) = A(s)/W_{\rho(s)}$;
2. exprimer les ThetaNullwerte sur $A'(s)$ en fonction des θ_{ji}.

Soit

$$\Omega = [\Omega_1\ \Omega_2] = \left[\begin{pmatrix} w_{11} & 0 & 0 \\ 0 & w_{12} & 0 \\ 0 & 0 & w_{13} \end{pmatrix} \begin{pmatrix} w_{21} & 0 & 0 \\ 0 & w_{22} & 0 \\ 0 & 0 & w_{23} \end{pmatrix} \right]$$

une matrice des périodes de $A = E_1 \times E_2 \times E_3$ et $\tau = \Omega_2^{-1}\Omega_1$. Le groupe $W = W_{\rho(s)} \subset A[2]$ étant symplectique, il existe une matrice $N \in \Gamma_3$ qui transforme W en le sous-groupe isotrope engendré par les $w_{1i}/2$. Dans cette nouvelle base, le quotient par W est alors "la division par 2" sur la matrice Ω_1. En notant

$$H = \begin{bmatrix} \frac{1}{2}\mathbf{1}_3 & 0 \\ 0 & \mathbf{1}_3 \end{bmatrix}$$

[8, Prop.4.1] montre que $\Omega' = \Omega N H$ est une matrice des périodes de $A'(s)$. Le calcul de la matrice N est développé dans la section [8, Sec.4.2].

Pour le second point, on procède en trois temps.

1. Posons $\tau' = {}^tN\tau = 2\boldsymbol{\tau}(\Omega')$. On couple les 36 ThetaNullwerte (paires) qui apparaissent dans le produit $\widetilde{\chi}_{18}(\boldsymbol{\tau}(\Omega')) = \widetilde{\chi}_{18}(\tau'/2)$ de telle manière qu'on puisse appliquer la formule de duplication (4.2). On obtient ainsi les expressions des produits de ThetaNullwerte en $\boldsymbol{\tau}(\Omega')$ en termes des ThetaNullwerte en τ'.
2. Pour chaque ThetaNullwert en τ', on applique la formule de transformation (4.1) pour obtenir une expression en terme d'une ThetaNullwert en τ.
3. Puisque τ est une matrice diagonale en les τ_i,

$$\theta[\boldsymbol{\varepsilon}](\tau) = \prod_{i=1}^{3} \theta \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} (\tau_i), \quad \text{pour toute caractéristique } [\boldsymbol{\varepsilon}] = \begin{bmatrix} a_1 b_1 c_1 \\ a_2 b_2 c_2 \end{bmatrix}.$$

Les calculs sont réalisés en partie avec MAGMA et détaillés dans la section [8, Sec.4.3]. On obtient *in fine* le résultat attendu.

Théorème 4.2.14 ([8, Th.4.1])**.** *Pour $s \in \mathbf{S}$ on a*

$$\chi := (2i\pi)^{54} \frac{\widetilde{\chi}_{18}(\boldsymbol{\tau}(\Omega'))}{(\det \Omega_2')^{18}} = X(s).$$

Ainsi $A'(s)$ est une jacobienne si et seulement si χ est un carré dans K.

Remarque 4.2.15. Il serait intéressant d'adapter les arguments précédents pour des sous-groupes isotropes maximaux de $A[n]$ avec $n > 2$. On obtiendrait ainsi d'autres expressions algébriques de l'obstruction de Serre.

4.3 Obstruction de Serre : le cas général

Cette partie expose les résultats de [3'] obtenus avec Gilles Lachaud et Alexey Zykin.

Dans cette partie, nous montrons que l'expression de χ dans le théorème 4.2.14 représente l'obstruction de Serre en général (Th. 4.3.7). Ce résultat est obtenu de manière assez conceptuelle comme la conséquence de résultats généraux d'Ichikawa (Prop.4.3.3) sur les formes $\widetilde{\chi}_h$ d'une part et sur la torsion des formes modulaires de Siegel géométriques (Cor.4.3.6) d'autre part. Cela nous permet de montrer qu'il n'y a pas de généralisation simple de la stratégie de Serre lorsque $g > 3$. Un autre résultat de l'article est de donner une démonstration nouvelle de la formule de Klein (Th. 4.3.10) en utilisant les morphismes naturels entre "formes modulaires de Siegel analytiques", "formes modulaires de Siegel géométriques", "formes modulaires de Teichmüller" et "invariants".

Remarquons que, parallèlement à nos travaux, Meagher [Mea08] a développé dans sa thèse une approche similaire de la stratégie de Serre.

4.3.1 Formes modulaires de Siegel et de Teichmüller

Les références sont [DM69],[Cha86], [FC90] et [vdG08]. Soient $g \geq 2$ un entier et A_g le champs des schémas abéliens principalement polarisés de dimension relative g. Soient $\pi : \mathsf{V}_g \longrightarrow \mathsf{A}_g$ le schéma abélien universel et $\pi_*\Omega^1_{\mathsf{V}_g/\mathsf{A}_g} \longrightarrow \mathsf{A}_g$ le fibré de rang g induit par les différentielles régulières relatives de V_g sur A_g. On note

$$\boldsymbol{\omega} = \bigwedge^g \pi_*\Omega^1_{\mathsf{V}_g/\mathsf{A}_g}.$$

Soient R un anneau commutatif et h un entier strictement positif. Une *forme modulaire de Siegel géométrique* de genre g et de poids h sur R est un élément du R-module

$$\mathbf{S}_{g,h}(R) = \Gamma(\mathsf{A}_g \otimes R, \boldsymbol{\omega}^{\otimes h}).$$

On procède de manière similaire pour les courbes. Soient M_g le champs de courbes lisses et propres de genre g. Soit $\pi : \mathsf{C}_g \longrightarrow \mathsf{M}_g$ la courbe universelle et $\boldsymbol{\lambda}$ le fibré inversible au-dessus de M_g défini par

$$\boldsymbol{\lambda} = \bigwedge^g \pi_*\Omega^1_{\mathsf{C}_g/\mathsf{M}_g}.$$

Une *forme modulaire de Teichmüller* de genre g et de poids h sur R est un élément de

$$\mathbf{T}_{g,h}(R) = \Gamma(\mathsf{M}_g \otimes R, \boldsymbol{\lambda}^{\otimes h}).$$

On suppose maintenant que $R = K$ est un corps. Pour une variété projective lisse X sur K, on note $\Omega^1_K[X] = H^0(X, \Omega^1_X \otimes K)$ le K-espace vectoriel des formes différentielles régulières sur X. Soit $(A, a) \in \mathsf{A}_g \otimes K$ une variété abélienne principalement polarisée de dimension g sur K (resp. $C \in \mathsf{M}_g \otimes K$ une courbe de genre g sur K). On note

$$\omega_K[A] \simeq \bigwedge^g \Omega^1_K[A] \quad (\text{resp. } \lambda_K[C] \simeq \bigwedge^g \Omega^1_K[C])$$

le K-espace vectoriel des sections de $\boldsymbol{\omega}$ (resp. $\boldsymbol{\lambda}$) sur (A,a) (resp. C). Pour $f \in \mathbf{S}_{g,h}(K)$ (resp. $f \in \mathbf{T}_{g,h}(K)$), et ω une base de $\omega_K[A]$ (resp. λ une base de $\lambda_K[C]$), on pose

$$f((A,a),\omega) = f(A,a)/\omega^{\otimes h} \in K, \quad (\text{resp. } f(C,\lambda) = f(C)/\lambda^{\otimes h} \in K).$$

Ainsi, une forme modulaire définit une règle qui fait correspondre à tout couple $((A,a),\omega)$ (resp. (C,λ)) un élément $f((A,a),\omega) \in K$ (resp. $f(C,\lambda)$) et qui ne dépend que de la classe de $\bar{K}$-isomorphisme du couple. Avec ces définitions, on a le résultat suivant (voir par exemple [Ich96]).

Proposition 4.3.1. *L'application de Torelli $t : \mathsf{M}_g \longrightarrow \mathsf{A}_g$, qui, à une courbe C, associe sa jacobienne $\operatorname{Jac} C$ avec sa polarisation canonique j, satisfait $t^*\boldsymbol{\omega} = \boldsymbol{\lambda}$, et induit pour tout corps K une application linéaire*

$$t^* : \mathbf{S}_{g,h}(K) = \Gamma(\mathsf{A}_g \otimes K, \boldsymbol{\omega}^{\otimes h}) \longrightarrow \mathbf{T}_{g,h}(K) = \Gamma(\mathsf{M}_g \otimes K, \boldsymbol{\lambda}^{\otimes h}).$$

Si C est définie sur K et $f \in \mathbf{S}_{g,h}(K)$, alors $[t^*f](C) = t^*[f(\operatorname{Jac} C, j)]$ c.-à-d. pour toute base ω de $\omega_K[\operatorname{Jac} C]$, on a

$$f((\operatorname{Jac} C, j), \omega) = [t^*f](C,\lambda) \qquad \text{si } t^*\omega = \lambda.$$

Supposons maintenant $R = K = \mathbb{C}$. On a alors un théorème de comparaison entre les formes modulaires de Siegel géométriques et analytiques introduites à la section 4.2.1 [FC90, p. 141].

Proposition 4.3.2. *Soient $f \in \mathbf{S}_{g,h}(\mathbb{C})$ et $\tau \in \mathbb{H}_g$. On pose*

$$\widetilde{f}(\tau) = (2i\pi)^{-gh} \cdot f(A_\tau, j)/(dz_1 \wedge \cdots \wedge dz_g)^{\otimes h}$$

où $(z_1, \dots z_g)$ est une base canonique de $\mathbb{C}^g$. L'application $f \mapsto \widetilde{f}$ est un isomorphisme de $\mathbf{S}_{g,h}(\mathbb{C})$ vers $\mathbf{R}_{g,h}(\mathbb{C})$.
De plus, si $\widetilde{f} \in \mathbf{R}_{g,h}(\mathbb{C})$ et $\Omega = [\Omega_1\ \Omega_2]$ est la matrice des périodes d'une variété abélienne principalement polarisée (A,a) sur $\mathbb{C}$ définie par une base ω_i de $\Omega^1_{\mathbb{C}}[A]$ et une base symplectique de $H_1(A,\mathbb{Z})$ pour a alors

$$f((A,a), \omega_1 \wedge \cdots \wedge \omega_g) = (2i\pi)^{gh} \cdot \frac{\widetilde{f}(\boldsymbol{\tau}(\Omega))}{\det \Omega_2^h}.$$

En particulier, à partir de la forme modulaire analytique $\widetilde{\chi}_h$ on définit une forme modulaire géométrique notée χ_h. Le résultat suivant dû à Ichikawa est un des deux résultats clés pour notre démonstration (voir [Ich96, Prop.3.4] et [Ich00]).

Proposition 4.3.3. *Soit $g \geq 3$. La forme modulaire de Siegel géométrique χ_h appartient à $\mathbf{S}_{g,h}(\mathbb{Z})$. De plus, il existe une forme modulaire de Teichmüller $\mu_{h/2} \in \mathbf{T}_{g,h/2}(\mathbb{Z})$ telle que*

$$t^*(\chi_h) = (\mu_{h/2})^2. \tag{4.3}$$

Remarque 4.3.4. La première partie découle de la rationalité des coefficients du développement en série de Fourier de χ_h et de [FC90, V.1]. La seconde partie est une amélioration de [Tsu91].

On suppose maintenant que gh est pair (sinon $\mathbf{S}_{g,h}(K) = \{0\}$) et $\operatorname{car} K \neq 2$. De l'invariance de f dans la classe de $\bar{K}$-isomorphisme du couple $((A,a),\omega)$, on déduit le second résultat essentiel pour la démonstration.

Proposition 4.3.5 ([3', Cor1.2.2])**.** *Soient (A,a) une variété abélienne principalement polarisée de dimension g définie sur un corps K et $f \in \mathbf{S}_{g,h}(K)$. Soient $\omega_1,\dots,\omega_g$ une base de $\Omega^1_K[A]$ et $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \omega_K[A]$. Alors*

$$\bar{f}(A,a) = f((A,a),\omega) \pmod{K^{*h}} \in K/K^{*h}$$

ne dépend pas du choix d'une base de $\Omega^1_K[A]$. En particulier $\bar{f}(A,a)$ est un invariant de la classe d'isomorphisme de (A,a).

Corollaire 4.3.6 ([3', Cor[1.2.3])**.** *On suppose g impair et $f \in \mathbf{S}_{g,h}(K)$. Soit (A',a') une tordue quadratique non triviale de (A,a). Il existe $c \in K \setminus K^2$ tel que*

$$\bar{f}(A,a) = c^{h/2}\bar{f}(A',a').$$

Ainsi, si $\bar{f}(A,a) \neq 0$, les représentants $\bar{f}(A,a)$ et $\bar{f}(A',a')$ n'appartiennent pas à la même classe de K^*/K^{*h}.

4.3.2 Application à l'obstruction de Serre

En genre 3, avec les notations du paragraphe 4.2.1, on a le résultat suivant qui généralise le théorème 4.2.14.

Théorème 4.3.7 ([3', Th.1.3.3])**.** *Soit (A,a) une variété abélienne principalement polarisée de dimension 3 sur $K \subset \mathbb{C}$. Soient $\omega_1,\omega_2,\omega_3$ une base de $\Omega^1_K[A]$ et $\gamma_1,\dots,\gamma_6$ une base symplectique de $H_1(A,\mathbb{Z})$ pour la polarisation a. Soient $\Omega = [\Omega_1\ \Omega_2]$ la matrice des périodes définie par ces bases et $\tau = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_3$.*

1. *Si $\widetilde{\Sigma}_{140}(\tau) = 0$ et $\widetilde{\chi}_{18}(\tau) = 0$ alors (A,a) est décomposable sur $\bar{K}$. En particulier ce n'est pas une jacobienne.*
2. *Si $\widetilde{\Sigma}_{140}(\tau) \neq 0$ et $\widetilde{\chi}_{18}(\tau) = 0$ alors il existe une courbe hyperelliptique C/K telle que $(\operatorname{Jac} C, j) \simeq (A,a)$.*
3. *Si $\widetilde{\chi}_{18}(\tau) \neq 0$ alors (A,a) est isomorphe à la jacobienne d'une courbe (non hyperelliptique) si et seulement si*

$$\chi := \chi_{18}((A,a),\omega) = (2i\pi)^{54} \cdot \frac{\widetilde{\chi}_{18}(\tau)}{\det \Omega_2^{18}}$$

est un carré dans K,avec $\omega = \omega_1 \wedge \omega_2 \wedge \omega_3 \in \omega_K[A]$.

Les résultats géométriques des points ci-dessus proviennent du théorème d'Igusa et (2) est la conséquence immédiate du théorème 4.1.4. Pour (3), la condition nécessaire provient du résultat d'Ichikawa 4.3.3. La réciproque se démontre grâce au corollaire 4.3.6 sur la torsion.

4.3.3 Application à la formule de Klein

Pour retrouver la formule de Klein, qui relie le discriminant des quartiques et $\widetilde{\chi}_{18}$, nous introduisons tout d'abord la notion d'invariant géométrique.

Soient m un entier et K un corps algébriquement clos de caractéristique première à m. Soit X_m (resp. X_m^0) l'ensemble des formes ternaires F de degré m définies sur K (resp. et de discriminant non nul). Soit

$$\mathsf{Y}_m^0 = \{(F,x) \in \mathsf{X}_m^0 \times \mathbb{P}^2,\ F(x) = 0\}$$

la courbe universelle au-dessus de X_m^0 Pour tout $F \in \mathsf{X}_m^0$, la courbe $C_F : F = 0$ est une courbe lisse de genre $g = \binom{m-1}{2}$ dont on peut écrire une base canonique de différentielles régulières comme suit [BK86, p.630]. Soit

$$\eta^{(1)} = \frac{f(x_2dx_3 - x_3dx_2)}{q_1}, \quad \eta^{(2)} = \frac{f(x_3dx_1 - x_1dx_3)}{q_2}, \quad \eta^{(3)} = \frac{f(x_1dx_2 - x_2dx_1)}{q_3},$$

où les q_i sont les dérivées partielles de F et $f \in \mathsf{X}_{m-3}$. Les formes $\eta^{(i)}$ se recollent pour donner une différentielle régulière $\eta_f(F)$ sur $\Omega^1_K[C_F]$. Soit $\eta_1, \ldots, \eta_g$ une base de $\Omega^1_K[C_F]$ obtenue en substituant à f la base canonique de X_{m-3} et $\eta = \eta_1 \wedge \cdots \wedge \eta_g$ la section de

$$\boldsymbol{\alpha} = \bigwedge^g \pi_* \Omega^1_{\mathsf{Y}_m^0/\mathsf{X}_m^0}.$$

On a la comparaison suivante entre invariants et invariants géométriques.

Proposition 4.3.8 ([3', Prop.2.1.2])**.** *Soient h un entier et $\mathbf{I}$ l'anneau gradué des invariants des fonctions régulières sur X_m^0 sous l'action classique de $\mathrm{SL}_3(K)$. L'application linéaire*

$$\Phi \mapsto \rho(\Phi) = \Phi \cdot \eta^{\otimes h}$$

est un isomorphisme de

$$\rho : \mathbf{I}_{gh}(\mathsf{X}_m^0) \xrightarrow{\sim} \Gamma(\mathsf{X}_m^0, \boldsymbol{\alpha}^{\otimes h})^{\mathrm{GL}_3(K)}.$$

Avec cette interprétation, il est alors possible de comparer les invariants et les formes modulaires de Teichmüller en utilisant le morphisme $p : \mathsf{X}_m^0 \longrightarrow \mathsf{M}_g$.

Proposition 4.3.9 ([3', Prop.2.2.1])**.** *Pour tout entier $h \geq 0$, l'application linéaire $\sigma = \rho^{-1} \circ p^*$ est un morphisme de :*

$$\mathbf{T}_{g,h}(K) \longrightarrow \mathbf{I}_{gh}(\mathsf{X}_m^0)$$

tel que

$$\sigma(f)(F) = f(C_F, \lambda) \text{ avec } \lambda = (p^*)^{-1}\eta,$$

pour tout $F \in \mathsf{X}_d^0$ et tout $f \in \mathbf{T}_{g,h}(K)$. Si $m = 4$ (et $g = 3$), σ est un isomorphisme.

Nous sommes maintenant en mesure d'énoncer le résultat de Klein [Kle90, Eq.118,p.462].

Théorème 4.3.10 ([3', Th.2.2.3]). *Soient $F \in \mathsf{X}_4^0(\mathbb{C})$ et $C_F : F = 0$ une quartique lisse. Soit (η_1, η_2, η_3) la base des différentielles de $\Omega^1_{\mathbb{C}}[C_F]$ définie ci-dessus et $(\gamma_1, \dots \gamma_6)$ une base symplectique de $H_1(C_F, \mathbb{Z})$ pour le couplage d'intersection. Soit $\Omega = [\Omega_1\ \Omega_2]$ la matrice des périodes C_F definie par ces bases et $\tau = \boldsymbol{\tau}(\Omega)$. Alors*

$$\mathrm{Disc}(F)^2 = (2i\pi)^{54} \cdot \frac{\widetilde{\chi}_{18}(\tau)}{\det(\Omega_2)^{18}}.$$

La démonstration procède comme suit. Grâce aux propositions précédentes, la fonction $I = \sigma \circ t^*(\chi_{18})$ est un invariant. Comme il ne s'annule pas sur X_4^0 (Th. 4.2.6) et que le discriminant est absolument irréductible, c'est une puissance du discriminant. On conclut en comparant les poids.

Remarque 4.3.11. Le théorème précédent montre que

$$\mu_9(C_F, \lambda) = \pm \mathrm{Disc}\, F.$$

Cette formule peut peut-être se déduire directement de la définition de μ_9 [Ich95, p.1059]. Cela demanderait de décrire explicitement l'isomorphisme de Mumford pour les quartiques planes. Cela a été fait pour les courbes hyperelliptiques dans [dJ07].

4.3.4 Généralisation en genre $g > 3$

Puisque l'obstruction de Serre est un phénomène qui apparaît en tout genre $g \geq 3$, nous pouvons nous interroger sur la généralisation de la stratégie de Serre. Pour être en mesure d'appliquer le corollaire 4.3.6, il nous faut supposer g impair. Mais même dans ce cas, puisque la valuation 2-adique de $h/2$ est $g - 3 > 0$, il ne suffit plus que χ_h soit un carré pour faire la distinction entre A et sa tordue quadratique. Nous aurions plutôt besoin d'une racine 2^{g-2}-ième et d'après [Tsu91, Th.1], $t^*(\chi_h)$ n'admet pas de racine quatrième.

Question : Peut-on trouver une forme modulaire pour remplacer (ou compléter) χ_h ?

L'autre aspect est la généralisation de la formule de Klein. Dans le cas hyperelliptique, des expressions analytiques du discriminant sont connues [Guà02], [Loc94]. Dans le cas non hyperelliptique de genre 4, un renvoi de bas de page [Kle90, p.462] donne, sans démonstration, la jolie formule suivante

$$\frac{\widetilde{\chi}_{68}(\boldsymbol{\tau}(\Omega))}{\det(\Omega_2)^{68}} = c \cdot \Delta(C)^2 \cdot T(C)^8$$

où $\Omega = [\Omega_1\ \Omega_2]$ est une matrice des périodes d'une courbe de genre 4 non hyperelliptique, plongée canoniquement dans $\mathbb{P}^3$ comme l'intersection d'une quadrique Q et d'une surface cubique E. Les éléments $\Delta(C)$ et $T(C)$ sont respectivement le discriminant de Q et le

tact-invariant de Q et E [Sal65, p.122]. Enfin c est une constante non précisée.

Question : Peut-on donner une démonstration de cette formule et généraliser en tout genre ?

4.4 Calcul de l'obstruction et courbes optimales

Cette partie décrit les résultats obtenus dans [7'].

À la suite des résultats obtenus dans la partie précédénte, il restait à comprendre comment calculer effectivement l'obstruction pour des courbes de genre 3 sur un corps fini. Ceci comporte deux étapes. Tout d'abord, une étape théorique où il faut montrer que l'obstruction se comporte bien par relèvement, puis réduction. C'est l'objet de la section 4.4.1. Puis, une seconde étape dans laquelle il s'agit de relever effectivement la variété abélienne et sa polarisation, décrite en terme de forme hermitienne. C'est ce qu'on explique dans la section 4.4.2.

Cette procédure, si elle permet de résoudre des cas particuliers, est très coûteuse en terme de temps de calcul et ne peut pas être aisément systématisée. Il serait intéressant d'obtenir des résultats algébriques sur les diviseurs de χ_{18}. Les tableaux de la section 4.4.3 présentent des données pour étayer de futures conjectures. On renvoie aussi à la section 4.5.1 pour quelques pistes.

Notations et conventions pour la partie. La lettre K désigne un sous-corps de $\mathbb{C}$. La lettre $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ désigne un corps fini de caractéristique différente de 2.

4.4.1 Obstruction de Serre sur les corps finis

La section 4.3.1 montre que la plupart des éléments dont nous avons eu besoin pour la démonstration du théorème 4.3.7, en particulier l'existence des formes χ_{18} et μ_9, sont valables en toute caractéristique différente de 2. Seul le théorème d'Igusa n'a *a priori* de sens que sur $\mathbb{C}$. Pour obtenir les arguments géométriques sur les corps finis, nous utilisons les deux faits suivants. La forme modulaire $\widetilde{\chi}_{18}$ est nulle sur $(\mathsf{A}_3 \setminus t(\mathsf{M}_3)) \otimes \mathbb{C}$, donc χ_{18} est nulle si la variété abélienne principalement polarisée de dimension 3, $(A, a)/k$, est décomposable sur $\bar{k}$. De plus, la comparaison de χ_{18} avec la forme de Teichmüller μ_9 et la définition de celle-ci [Ich95, p.1059] montrent que, si $\chi_{18} \neq 0$, alors (A, a) est géométriquement la jacobienne d'une courbe non hyperelliptique (pour les autres implications du théorème d'Igusa, voir section 4.5.1).

Proposition 4.4.1 ([7', Prop.2.3])**.** *Soit (A, a) une variété abélienne de dimension 3 principalement polarisée définie sur k. Soit $(\omega_1, \omega_2, \omega_3)$ une base de $\Omega^1_k[A]$ et soit $\omega = \omega_1 \wedge \omega_2 \wedge \omega_3$. La variété (A, a) est la jacobienne d'une courbe de genre 3 non hyperelliptique*

si et seulement si $\chi_{18}((A,a),\omega)$ *est un carré non nul dans* k*. De plus, si* $\chi_{18}((A,a),\omega)$ *n'est pas un carré alors* (A,a) *n'est pas une jacobienne.*

Malheureusement, on ne sait pas calculer directement la valeur de χ_{18} sur le corps fini. Comme suggéré par Serre dans sa lettre à Top, on procède par relèvement sur $\mathbb{C}$. On calcule alors la valeur de χ_{18} par sa formule analytique, puis on réduit le résultat sur le corps fini. La proposition suivante montre qu'une telle procédure calcule effectivement l'obstruction.

Proposition 4.4.2 ([7', Prop.2.4])**.** *Soient* (A,a) *une variété abélienne de dimension* 3 *principalement polarisée définie sur* k *et* $(\tilde{A},\tilde{a})$ *un relèvement de* (A,a) *sur un anneau local* S *d'un corps de nombres* K *de corps résiduel* k *(un tel relèvement existe toujours). Pour tout choix d'une base de différentielles régulières* $(\omega_1,\omega_2,\omega_3) \in \Omega^1_S[\tilde{A}]$ *et d'une base symplectique de* $H_1(\tilde{A}\otimes K,\mathbb{Z})$ *pour* a*, on note* $\Omega = [\Omega_1\ \Omega_2]$ *la matrice des périodes ainsi définie. Alors*

$$\chi := \chi_{18}((\tilde{A},\tilde{a}),\omega_1\wedge\omega_2\wedge\omega_3) = \frac{(2\pi)^{54}}{2^{28}}\cdot\frac{\prod_{\boldsymbol{\varepsilon}}\theta[\boldsymbol{\varepsilon}](\boldsymbol{\tau}(\Omega))}{\det(\Omega_2)^{18}} \tag{4.4}$$

appartient à S*. Soit* $\mathfrak{p}$ *tel que* $k = S/\mathfrak{p}$*, alors* (A,a) *est la jacobienne d'une courbe non hyperelliptique de genre* 3 *si et seulement si* $\chi \pmod{\mathfrak{p}}$ *est un carré non nul dans* k*. De plus si* $\chi \pmod{\mathfrak{p}}$ *n'est pas un carré dans* k *alors* (A,a) *n'est pas une jacobienne.*

4.4.2 Calcul explicite : un exemple

Afin de réaliser le calcul de l'obstruction, il nous faut être en mesure de contrôler la polarisation sur A et d'en calculer la première classe de Chern sur le relèvement. Comme les classes d'isogénie des courbes optimales contiennent la puissance d'une courbe elliptique E, on se concentre sur le cas $A = E^g$ et on utilise un formalisme proche de la section 3.3.2 mais E est cette fois ordinaire. Plus précisément, soit

$$E : y^2 + a_1xy + a_3y = f(x) \text{ avec } f \in K[x],$$

une courbe elliptique dont tous les endomorphismes sont définis sur K. On suppose de plus que $\mathrm{End}(E)$ est un ordre $\mathcal{O}$ de l'anneau des entiers $\mathcal{O}_L$ d'un corps quadratique imaginaire L. On note $\omega_E = dx/(2y + a_1x + a_3)$ une différentielle régulière sur E et a_0 la polarisation produit sur E^g. En identifiant $\mathrm{End}(E) \simeq \mathbf{M}_g(\mathcal{O})$, l'involution de Rosati $\dagger$ est $M \mapsto {}^t\bar{M}$ où $\bar{}$ est la conjugaison complexe. Classiquement [Mum08, p.209], le morphisme $M \mapsto a_0M$ définit une bijection entre les matrices hermitiennes définies positives de déterminant 1 de $\mathbf{M}_g(\mathcal{O})$ et les polarisations principales sur E^g.

Remarque 4.4.3. Lorsque K est un corps fini et que $\mathrm{End}(E) = \mathcal{O}_L = \mathbb{Z}[\pi]$, Serre [Lau02] donne une équivalence de catégorie entre les éléments A de la classe d'isogénie de E^g et les modules hermitiens sur $\mathcal{O}_L$. Notre formalisme est "dual" du formalisme de Serre et les deux coïncident lorsque $A = E^g$ (voir [7', Sec.3.2]).

Illustrons maintenant le calcul de l'obstruction sur un exemple. Existe-t-il une courbe C optimale de genre 3 sur $k = \mathbb{F}_{47}$? Nous savons que si tel est le cas $\operatorname{Jac} C \sim E^3$ où E/k est une courbe elliptique de trace $-\lfloor 2\sqrt{47} \rfloor = -13$. La courbe E est donc ordinaire et son anneau des endomorphismes contient $\mathbb{Z}[\pi] \simeq \mathbb{Z}[(13 + \sqrt{13^2 - 4 \cdot 47})/2] = \mathbb{Z}[\tau]$ avec $\tau = (1 + \sqrt{-19})/2$. Ainsi, $\operatorname{End}(E) = \mathbb{Z}[\pi]$ est l'anneau des entiers $\mathcal{O}_L$ de $L = \mathbb{Q}(\sqrt{-19})$. Dans l'idée de démontrer l'existence de C, on peut supposer que $\operatorname{Jac} C \simeq E^3$ avec E une telle courbe. En fait, puisque $\mathcal{O}_L$ est principal, E est unique et [Lau02, Appendix] montre que, si $A \sim E^3$, alors $A \simeq E^3$.
Grâce aux travaux de [Sch98], on sait qu'il existe une unique matrice hermitienne $M \in \mathbf{M}_3(\mathcal{O}_L)$ définie positive de déterminant 1, à équivalence près,

$$M = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\bar{\tau} & 3 \end{pmatrix},$$

qui soit de plus *indécomposable* (c.-à-d. non équivalente à une matrice diagonale par blocs). Ceci est une condition nécessaire et suffisante pour que la polarisation associée soit absolument indécomposable [Lau02, Appendix]. Encore une fois, il n'est pas utile de le vérifier : si la valeur de χ_{18} est non nulle alors nous savons que la polarisation est indécomposable. On choisit un relèvement canonique de E, par exemple

$$\tilde{E} : y^2 = x^3 - 152x - 722.$$

La section [7', 3.3] montre comment trouver une matrice des périodes pour $(\tilde{E}^3, a_0 M)$ par rapport aux pull-backs ω_i sur $\tilde{E}^3$ des différentielles $\omega_{\tilde{E}}$ sur les $\tilde{E}$. Si on note $[w_1\ w_2]$ une matrice des périodes de $\tilde{E}$ par rapport à la différentielle $\omega_{\tilde{E}}$, alors la première classe de Chern de $a_0 M$ est donnée par

$$H = c_1(a_0 M) = \frac{1}{\operatorname{Im}(w_1 \bar{w}_2)} {}^t M.$$

Si on pose

$$\Omega_0 = \left[\begin{pmatrix} w_1 & 0 & 0 \\ 0 & w_1 & 0 \\ 0 & 0 & w_1 \end{pmatrix} \begin{pmatrix} w_2 & 0 & 0 \\ 0 & w_2 & 0 \\ 0 & 0 & w_2 \end{pmatrix} \right],$$

la forme alternée T associée à H sur le réseau $\Omega_0 \mathbb{Z}^{2g}$ est $T = \operatorname{Im}({}^t\Omega_0 H \bar{\Omega}_0)$. On calcule alors une matrice $B \in \mathbf{M}_6(\mathbb{Z})$ telle que $B T {}^t B = \mathbf{J}_3$ et $\Omega = \Omega_0 {}^t B$ est une matrice des périodes pour une base symplectique de $H_1(\tilde{E}^3, \mathbb{Z})$ et les différentielles ω_i. Nous sommes ainsi en mesure de calculer une approximation de

$$\chi = \chi_{18}((\tilde{E}^3, a_0 M), \omega_0) \text{ avec } \omega_0 = \omega_1 \wedge \omega_2 \wedge \omega_3$$

grâce à la formule analytique (4.4), puis de la reconnaître comme un élément de L. On trouve ici

$$\chi = (2^{19} \cdot 19^7)^2.$$

Ainsi χ est un carré dans k et il existe une courbe optimale de genre 3 sur k.

TABLE 4.1 – Modèle de Gross $E(d)$

d	modèle	discriminant
7	$y^2+xy=x^3-x^2-2x-1$	-7^3
19	$y^2+y=x^3-2\cdot 19x+\frac{19^2-1}{4}$	-19^3
43	$y^2+y=x^3-2^2\cdot 5\cdot 43x+\frac{3\cdot 7\cdot 43^2-1}{4}$	-43^3
67	$y^2+y=x^3-2\cdot 5\cdot 11\cdot 67x+\frac{7\cdot 31\cdot 67^2-1}{4}$	-67^3
163	$y^2+y=x^3-2^2\cdot 5\cdot 23\cdot 29\cdot 163x+\frac{7\cdot 11\cdot 19\cdot 127\cdot 163^2-1}{4}$	-163^3

Remarque 4.4.4. En faisant varier p, on trouve qu'il existe une courbe optimale pour $q=47,61,137,277$ [7', Cor.4.1].

4.4.3 Quelques valeurs de l'obstruction

Avec les choix de la section précédente, on peut donner les valeurs de

$$\chi=\chi_{18}((\tilde{E}^3,a_0M),\omega_0)$$

pour différents $\mathcal{O}_L$, avec $L=\mathbb{Q}(\sqrt{-d})$, en particulier ceux de nombre de classes 1. D'après [Hof91, p.418], il n'existe pas de forme hermitienne M, définie positive de déterminant 1, dans $\mathbf{M}_3(\mathcal{O}_L)$ pour $d=3,4,8,11$. On considère donc les cas $d=7,19,43,67,163$ (pour 163, comme il y a plus de 100 choix possibles pour M à équivalence près, nous n'avons considéré que deux cas). Nous choisissons pour modèles pour $\tilde{E}$, les modèles de Gross $E(d)$ qui sont les courbes CM par $\mathcal{O}_L$ de discriminant minimal que nous rappelons dans le tableau 4.1.

Nous discuterons du bien fondé d'un tel choix dans le section 4.5.1. Notons simplement que le choix de ces courbes elliptiques est naturel dans notre contexte car il existe une formule très simple [7', Lem.4.1] donnant la trace de leur réduction modulo p (et pas seulement au signe près). Les résultats pour les différents M possibles sont donnés dans [7', Tab.2] et [7', Tab.3].

Remarque 4.4.5. On peut aussi réaliser ce calcul lorsque $\mathcal{O}_L$ n'est pas principal. Voici un exemple avec nombre de classes 2 [7', Rem.3] : soient

$$E(15):y^2=x^3+\left(\frac{15}{32}+\frac{219}{32}\sqrt{5}\right)x-\left(\frac{77}{16}+\frac{385}{32}\sqrt{5}\right)$$

qui est CM par $\sqrt{-15}$ et la forme 15 (dim.3.1) #2 (avec la classification issue des tables de Schiemann sur le web)

$$M=\begin{pmatrix}2 & -1 & -1+\bar{\tau}\\ -1 & 2 & 1-\bar{\tau}\\ -1+\tau & 1-\tau & 3\end{pmatrix},\quad \tau=\frac{1+\sqrt{-15}}{2}.$$

On obtient

$$\chi=22769095299822142340569171645771726299/4+101825226030208344848630851512443226 75\cdot\sqrt{5}/4$$
$$+44626409093538218819956956474294768 69\cdot\sqrt{-15}/4+99783306179228864438239827551142024 45\cdot\sqrt{-3}.$$

La groupe des automorphismes de la courbe correspondante est d'ordre 24.

Nous présentons dans le tableau 4.2 les valeurs extraites des tableaux de l'article qui appartiennent à $\mathbb{Q}$ (et pas seulement à L).

Remarque 4.4.6. Comme me l'a suggéré Serre, on peut considérer pour chaque d et chaque bonne matrice M (indexée dans le tableau 4.2 par $\#i$), une courbe $E_{d,i}$ qui est la tordue quadratique de $E(d)$ par le facteur δ non carré de χ. Ce faisant, on obtient que

$$\chi_{18}((E^3_{d,i}, a_0 M), \omega_0) = \delta^{27} \cdot \chi$$

est maintenant un carré dans L. Il existe donc une courbe de genre 3, notée $X_{d,i}$, définie sur L tel que $(\operatorname{Jac} X_{d,i}, j) = (E^3_{d,i}, a_0 M)$. Par exemple dans le cas $19, \#1$, la courbe $E_{19,1}$ est la courbe $y^2 = x^3 - 152x - 722$ (celle que nous avions déjà considérée dans l'exemple $\mathbb{F}_{47}$). En utilisant les constructions de [Guà09], il est même possible de calculer un modèle de $X_{d,i}$ sur L. Lorsque M est unique, comme c'est le cas pour $d = -19$, la courbe $X_{d,i}$ descend sur $\mathbb{Q}$. Après calculs, on trouve [7', ex.1]

$$X_{19,1} : x^4 + (1/9)y^4 + (2/3)x^2y^2 - 190y^2 - 570x^2 + (152/9)y^3 - 152x^2y - 1083 = 0.$$

Bien sûr la courbe $X_{7,1}$ n'est rien d'autre que la courbe de Klein $x^3y + y^3z + z^3x = 0$. Dans l'article, on donne aussi l'exemple de la courbe $X_{43,3}$.

TABLE 4.2 – Quelques valeurs rationnelles de χ

d	M	$\chi := \chi_{18}((A, a_0M), \omega_0)$	$\#\operatorname{Aut}(A, a_0M)$
7, # 1	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \bar{\tau} \\ 1 & \tau & 2 \end{pmatrix}$	$(7^7)^2$	$2 \cdot 168$
19 # 1	$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\bar{\tau} & 3 \end{pmatrix}$	$(2^5 \cdot 19^7)^2 \cdot (-2)$	$2 \cdot 6$
43, # 1	$\begin{pmatrix} 3 & 1 & 1-\bar{\tau} \\ 1 & 4 & 2 \\ 1-\tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 43^7)^2 \cdot (-47 \cdot 79 \cdot 107 \cdot 173)$	$2 \cdot 1$
43, # 2	$\begin{pmatrix} 3 & 1+\bar{\tau} & 2-\bar{\tau} \\ 1+\tau & 5 & 2-\bar{\tau} \\ 2-\tau & -2-\tau & 5 \end{pmatrix}$	$(2^5 \cdot 3^4 \cdot 43^7)^2 \cdot (-2 \cdot 3 \cdot 7)$	$2 \cdot 6$
43, # 3	$\begin{pmatrix} 2 & -1 & 1 \\ -1 & 4 & 1+\bar{\tau} \\ 1 & 1-\tau & 4 \end{pmatrix}$	$(2^6 \cdot 5^3 \cdot 43^7)^2 \cdot (-487)$	$2 \cdot 2$
67, # 3	$\begin{pmatrix} 5 & -2+\bar{\tau} & -1-\bar{\tau} \\ -2+\tau & 6 & -2 \\ -1-\tau & -2 & 7 \end{pmatrix}$	$(2^6 \cdot 3^6 \cdot 67^7)^2(-13 \cdot 53 \cdot 71 \cdot 131 \cdot 3319)$	$2 \cdot 1$
67, # 6	$\begin{pmatrix} 5 & -1+\bar{\tau} & \bar{\tau} \\ -1+\tau & 5 & 2 \\ \tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 5^3 \cdot 67^7)^2 \cdot 83 \cdot 211 \cdot 1637 \cdot 2441$	$2 \cdot 1$
67, # 7	$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 3 & -2+\bar{\tau} \\ -1 & -2+\tau & 7 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 67^7)^2 \cdot (-2 \cdot 7 \cdot 31)$	$2 \cdot 6$
67, # 11	$\begin{pmatrix} 5 & \bar{\tau} & -2 \\ \tau & 6 & 2+\bar{\tau} \\ -2 & 2+\tau & 6 \end{pmatrix}$	$(2^6 \cdot 3^4 \cdot 5^3 \cdot 67^7)^2 \cdot (-3 \cdot 7 \cdot 8731)$	$2 \cdot 2$
67, # 13	$\begin{pmatrix} 3 & 1 & -1 \\ 1 & 5 & -3+\bar{\tau} \\ -1 & -3+\tau & 5 \end{pmatrix}$	$(2^8 \cdot 5^4 \cdot 67^7)^2 \cdot (-2 \cdot 5 \cdot 9769)$	$2 \cdot 2$
163, # 85	$\begin{pmatrix} 2 & 1 & -\bar{\tau} \\ 1 & 2 & 1-\bar{\tau} \\ -\tau & 1-\tau & 28 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 11^4 \cdot 163^7)^2 \cdot (-2 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$	$2 \cdot 6$

4.5 Projet de recherche

Ce projet de recherche se scinde en trois parties. La première est dans le prolongement des articles de ce chapitre. On s'intéresse en particulier au problème des diviseurs de χ_{18}. La deuxième partie présente une alternative géométrique à l'approche de Serre. Elle contient une généralisation des constructions de [HLP00] présentée dans la section 4.2.2. La dernière partie explore les relations explicites sur $\mathbb{C}$ entre la courbe et sa jacobienne.

4.5.1 Une formule algébrique pour χ_{18} ?

Je souhaite poursuivre mon travail autour de l'approche de Serre sur plusieurs niveaux. Tout d'abord, sur un plan technique, j'aimerais clarifier certains aspects de l'équivalence de catégories de Serre entre variétés abéliennes et modules hermitiens. Comment obtient-on en général la première classe de Chern d'une polarisation décrite par une forme hermitienne sur le module ? Peut-on se passer de certaines des hypothèses de la remarque 4.4.3 ? Quelles sont les relations avec la théorie générale de Howe (point (6) de la section 3.1) qui utilise, dans le cas ordinaire, le relèvement canonique ? Avec notre approche ? Peut-on trouver un analogue de l'invariant de Humbert généralisé, développé par Kani [Kan08] en genre 2 ?
Il est également notable que les valeurs de χ que nous obtenons dans le tableau 4.2 sont entières. Intuitivement, ceci est dû au fait que les modèles $E(d)$ définissent un schéma semi-abélien sur $\mathbb{Z}$ et donc un point de $\bar{\mathsf{A}}_3 \otimes \mathbb{Z}$, pour une bonne compactification arithmétique de A_3. Mais ces idées restent à préciser.

Sur un autre plan, je souhaite m'intéresser à la question suivante. Supposons que E est une courbe elliptique sur un corps de nombres K, CM par l'anneau des entiers $\mathcal{O}_L$ d'un corps de nombres $L = \mathbb{Q}(\sqrt{-d})$ et $A \simeq E^3$ est une variété abélienne avec une polarisation principale absolument indécomposable $a = a_0 M$ pour $M \in \mathbf{M}_3(\mathcal{O}_L)$. Peut-on "lire" algébriquement la valeur de $\chi = \chi_{18}((A, a), \omega_0)$ à partir des coefficients de E et de M ? Puisqu'à travers la formule de Klein, χ_{18} est lié au discriminant, nous cherchons une formule de Néron-Ogg-Shafarevich pour A [Sil92, Appendix C,§16].
Pour simplifier, nous commencerons avec le genre 2. La formulation est identique, avec $M \in \mathbf{M}_2(\mathcal{O}_L)$ et on a une relation similaire entre la forme modulaire χ_{10}^2 et le discriminant de la courbe (voir Sec. 4.2.1). Deux types de travaux pourront servir de sources d'inspiration. Les premiers [Sai89],[Ünv04], [Liu94] sont très généraux et expriment le discriminant à partir de données sur un modèle de la courbe. Il n'est pas clair comment obtenir toutes ces informations à partir de E et de M. Les seconds [GL07],[GL06],[dSG97] étudient le cas des surfaces abéliennes CM, qui est en quelque sorte "complémentaire" de notre cas.
En genre 3, une difficulté supplémentaire apparaît. La présence d'un premier divisant χ ne signifie plus nécessairement que la réduction n'est plus géométriquement une jacobienne (car elle a mauvaise réduction ou réduction décomposable) mais elle peut être la jacobienne d'une courbe hyperelliptique. C'est le cas par exemple, après une extension quadratique, pour les courbes $X_{7,1}$ et $X_{19,1}$, respectivement en caractéristique 7 et

19. En effet, le théorème d'Igusa 4.2.6 nous montre qu'il faut également considérer la forme $\widetilde{\Sigma}_{140}$. Nous avons vu au début de la section 4.4.1 comment obtenir certaines des implications de de ce théorème en caractéristique quelconque. Pour obtenir toutes les équivalences, une condition nécessaire est que la forme géométrique associée Σ_{140} soit primitive (c.-à-d. non nulle modulo un premier quelconque), tout comme les formes χ_h [Ich96, Prop.3.4]. Un calcul dans l'esprit de *loc. cit.* montre que la forme

$$\Sigma_{140} = \frac{(2i\pi)^{140}}{2^{218}} \cdot \frac{\widetilde{\Sigma}_{140}(\tau_a)}{\det(\Omega_2)^{140}} (\omega_1 \wedge \omega_2 \wedge \omega_3)^{\otimes 140}$$

est primitive. Cependant, nous ne savons pas montrer que cette condition est suffisante. En attendant, il est tout de même possible d'obtenir certains résultats inconditionnels simples. Par exemple, si la réduction de A n'est pas géométriquement une jacobienne, alors la réduction de E est supersingulière. La réciproque est vraie pour la réduction en 2 car il n'existe pas de bonne forme quaternionique indécomposable pour $p = 2$ [Oor91a]. Comme on le voit, ce ne sont que des résultats très partiels et qui ne concernent même pas l'exposant avec lequel ces premiers interviennent. Pour illustrer la difficulté de l'entreprise, considérons le cas $d = 15$ et $p = 19$. Un premier $\mathfrak{p}$ au-dessus de p dans $K = \mathbb{Q}(\sqrt{-15}, \sqrt{5})$ est caractérisé par le choix du signe des racines de -3 et de 5 modulo 19. En utilisant la valeur de χ et les remarques précédentes, on a les résultats suivants

$\sqrt{-3}$	$\sqrt{5}$	$(E(15)^3, a_0 M) \pmod{\mathfrak{p}}$ est la jacobienne
-4	9	d'une courbe de défaut 3 non hyperelliptique
-4	-9	d'une courbe de défaut 3 non hyperelliptique
4	-9	d'une courbe de nombre de points $1 + q - 3m + 3$
4	9	d'une courbe hyperelliptique.

Un espoir vient toutefois d'une observation de Mestre sur nos valeurs de χ lorsque l'ordre $\#\operatorname{Aut}(A, a_0 M) = 2 \cdot 6$. Grâce à ces propres résultats [Mes], il conjecture que

$$\chi = 3^{-15} \cdot (j^{1/3} - 12)^4 \cdot \Delta^4 \cdot c_6,$$

où j est le j-invariant de la courbe E, Δ son discriminant et c_6 son "c-invariant" comme définis par [Sil92, p.46]. Il semblerait que ce cas apparaisse pour tout $d \equiv 3 \pmod 4$.

4.5.2 Une alternative géométrique à l'approche de Serre

Je développe dans [5'] une alternative à la stratégie analytique proposée par Serre et expliquée dans ce chapitre. Elle est basée sur des constructions géométriques "classiques" ([Rec93], [ACGH85, p.270-273], [Bru08]) que nous exploitons dans un contexte arithmétique. Soit (A, Θ) une variété abélienne de dimension 3 sur un corps K de caractéristique différente de 2 avec Θ le diviseur d'une polarisation principale absolument indécomposable que l'on suppose symétrique et rationnel. Pour $\alpha \in A(K) \setminus \{0\}$, et en dehors d'un sous-ensemble connu, la courbe $\tilde{X}_\alpha = \Theta \cap (\Theta + \alpha)$ est lisse, de genre 7 et possède une involution sans point fixe $j_\alpha : z \mapsto \alpha - z$. Si α n'est pas un point de 2-torsion et si

(A, Θ) est géométriquement la jacobienne d'une courbe de genre 3 non hyperelliptique, la courbe $X'_\alpha = \tilde{X}_\alpha / j_\alpha$ est une courbe de genre 4 non hyperelliptique. Elle se plonge canoniquement dans $\mathbb{P}^3$ comme l'intersection d'une unique quadrique Q' et d'une surface cubique. Notre premier résultat est de montrer que le discriminant de Q' est un carré dans K^* si et seulement si (A, Θ) est la jacobienne d'une courbe (non hyperelliptique) de genre 3. Si α est un point de 2-torsion, la structure est plus riche : elle possède une autre involution sans point fixe $t_\alpha : z \mapsto \alpha + z$. La courbe $X_\alpha = \tilde{X}_\alpha / t_\alpha$ est une courbe de genre 4 non hyperelliptique. Si Q est la quadrique associée à X_α, alors le discriminant de Q est un carré dans K^* (resp. 0) si et seulement si (A, a) est la jacobienne d'une courbe non hyperelliptique (resp. hyperelliptique).

Je souhaite affaiblir les hypothèses techniques que je fais pour obtenir ces résultats. En particulier, lorsque α est un point de 2-torsion, il serait souhaitable d'inclure certains cas dégénérés car cela permettrait d'obtenir des constructions effectives :

- on retrouve géométriquement les résultats obtenus dans Howe, Leprevost et Poonen (2000) et rappelés dans la section 4.2.2. Ceci donne une interprétation géométrique du théorème 4.2.11.
- on étend leurs résultats en construisant des courbes de genre 3 dont la jacobienne est isogène au produit d'une courbe elliptique et de la jacobienne d'une courbe de genre 2. Ce résultat pourrait être utilisé pour améliorer ceux de *loc. cit.* en construisant des courbes de genre 3 sur $\mathbb{Q}$ dont la jacobienne a un grand nombre de points de torsion rationnels. Il permettrait aussi plus de flexibilité dans le choix des variétés abéliennes dans la classe d'isogénie du cube d'une courbe elliptique et donc dans les expressions de l'obstruction de Serre.

4.5.3 Liens entre la courbe et sa jacobienne analytique

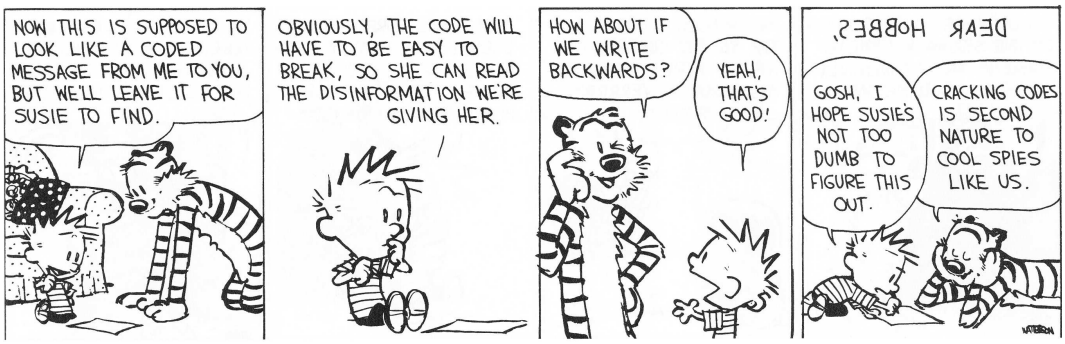
Pour de nombreuses applications, telles celles mentionnées dans la partie 2.5 ou la section 5.4.3, mais aussi certains problèmes de physique théorique [ER08], il est important de rendre explicites les relations entre une courbe C de genre $g > 0$ sur $\mathbb{C}$ et sa jacobienne. Nous allons donner quelques pistes sur ces questions (voir également la dernière partie de `http://iml.univ-mrs.fr/~ritzenth/slides/expo_ESF.pdf`).

1. Le passage de la courbe à sa jacobienne. Deux types de données sont intéressants. Le premier est une matrice des périodes de la jacobienne. Pour un modèle plan de la courbe, on sait réaliser ce type d'opérations en calculant les intégrales associées [DvH01]. À partir de cette matrice, on peut alors calculer les ThetaNullwerte en évaluant les séries qui les définissent. Ces opérations sont toutefois coûteuses. Il peut être préférable de les réaliser par une généralisation de la méthode de Gauss en genre 1 [Cox84]. Pour réaliser cela, plusieurs éléments sont nécessaires.
   - Tout d'abord, une formule donnant les ThetaNullwerte en fonctions des coefficients de la courbe. Dans le cas hyperelliptique (et à une racine quatrième près), c'est la formule de Thomae [Mum07]. En genre 3, dans le cas non hyperelliptique, la formule de Weber ([Web76], [6']) donne le quotient de deux ThetaNullwerte à

la puissance 4. Avec Nart, nous donnons une autre démonstration, plus simple, de cette formule [4']. Pour de nombreuses applications (construction CM, méthode AGM 2-adique), cette formule est suffisante mais nous avons besoin ici d'une expression pour les ThetaNullwerte (à la puissance 4) seules. Pour le genre $g > 3$, l'article [SB08] est un bon point de départ pour obtenir tout au moins les quotients des ThetaNullwerte.
   - Ensuite, définir des "bonnes racines" pour le calcul de l'AGM. En genre 2, [Dup06] a étudié cette question sous certaines hypothèses vérifiées expérimentalement. On pourra confronter son travail à celui de [Jar08].

2. Le passage de la jacobienne à sa courbe. On peut raisonner au niveau géométrique ou arithmétique. Supposons que l'on connaisse les quotients des ThetaNullwerte, ce qui a également une signification algébrique et peut être utilisé sur d'autres corps que $\mathbb{C}$.
   - Dans le cas hyperelliptique, géométriquement, la construction de la courbe se fait grâce aux formules de Rosehain.
   - Dans le cas non hyperelliptique, il est possible que les formules de [Web76, p.108], bien comprises, permettent de le faire également.

   Si le corps de base est $\mathbb{C}$ et que l'on connaît les fonctions thêta (en particulier leurs dérivées), on peut aussi utiliser les résultats de Guàrdia [Guà07] dans le cas hyperelliptique ou [Guà09] dans le cas du genre 3 non hyperelliptique. Ces méthodes permettent d'obtenir des modèles arithmétiques et ont été exploitées pour obtenir les courbes de la remarque 4.4.6. On pourra se demander s'il y a des généralisations de ces méthodes de reconstruction dans le cas non hyperelliptique de genre $g > 3$. Enfin, dans certains cas (par exemple la méthode complexe CM), on commence avec une matrice des périodes. Il faut donc calculer les ThetaNullwerte (et/ou leurs dérivées). Comme mentionné dans la section 5.4.3, en genre 1 et 2, ceci peut se faire de manière efficace, sous certaines hypothèses, en inversant la "fonction" l'AGM. La généralisation en tout genre est une question totalement ouverte.



5 Cryptographie

La cryptographie est un autre joli terrain de jeu pour les mathématiciens. On y rencontre des questions à l'énoncé souvent simple dont les réponses peuvent exiger des concepts mathématiques sophistiqués et parfois une vision originale d'un sujet qu'on croyait maintes fois visité. Les quatre parties ci-dessous s'inscrivent dans cette optique. Une fois décrite la motivation initiale, on passe sous silence la plupart des résultats purement cryptographiques, en privilégiant les questions mathématiques sous-jacentes. Ainsi, la partie 5.1 présente une loi d'addition géométrique sur la jacobienne d'une quartique plane lisse et considère la question de l'existence d'une droite, voire d'une tangente coupant cette quartique en des points rationnels uniquement. Dans la partie 5.2, on décrit une loi d'addition géométrique sur les courbes d'Edwards et son utilisation pour le calcul du couplage de Tate. On développe dans la section 5.2.3 un sujet de recherche sur la complétude pour les lois d'addition sur les variétés abéliennes. Dans la partie 5.3, on s'intéresse au couplage sur les courbes C de genre 2 supersingulières sur un corps fini k et on donne des générateurs de $\mathrm{End}_k^0(\mathrm{Jac}\, C)$ pour certaines courbes afin d'obtenir des applications de distorsion. Enfin, la dernière partie 5.4 expose une méthode de construction de courbes de genre 2 à multiplication complexe par relèvement 2-adique. La section 5.4.3 des réflexions sur les maints développements possibles.

Les parties étant relativement indépendantes, je ne présente pas de projet de recherche global. Néanmoins, on pourra trouver dans chaque partie des questions ouvertes et certaines pistes pour tenter d'y répondre.

5.1 Addition dans la jacobienne des courbes de genre 3

L'article de référence est [2] avec Stéphane Flon et Roger Oyono.

La méthode dite "AGM" fournit un algorithme polynomial pour le calcul du polynôme de Weil χ d'une courbe C de genre $1, 2$ ou 3 sur un corps fini k de caractéristique 2 [16]. Néanmoins, dans le cas du genre 3, cette méthode ne donne ce polynôme qu'au "signe près", c.-à-d. $\chi(\pm X)$. La technique habituelle pour lever l'indétermination consiste à prendre un point rationnel aléatoire $P \in (\mathrm{Jac}\, C)(k)$ et à vérifier si $\chi(1) \cdot P = 0$. La motivation initiale de l'article [2] était d'avoir un algorithme d'addition rapide pour les jacobiennes des quartiques planes lisses afin de mener à bien ce calcul final. Une autre source d'intérêt était la construction de cryptosystèmes efficaces en genre 3. À l'époque, les améliorations de l'attaque de la méthode de l'index (voir [CFA+06, Chap.21]) ne

concernaient pas le genre 3. Oyono [Oyo09] étudiait en particulier de tels systèmes basés sur des facteurs de dimension 3 des jacobiennes modulaires $J_0(N)$. Depuis, les développements récents ([Die06] pour les quartiques et [Smi08] dans le cas hyperelliptique), ont compromis l'avenir des courbes de genre 3 pour ce type d'applications. Il n'en reste pas moins que ces courbes peuvent être utiles pour les attaques par descentes et, ainsi, il apparaît nécessaire de disposer d'une arithmétique efficace dans la jacobienne.

Différents auteurs ont traité du problème de l'addition pour plusieurs familles de quartiques mais notre article était le premier à considérer le problème des quartiques en général. Une partie de l'article est consacrée à l'optimisation du nombre d'opérations dans les calculs. Nous renvoyons à [2, Sec.5] pour un historique et une comparaison avec les autres méthodes. Présentement, nous souhaitons exposer succinctement la méthode géométrique d'addition ainsi que les questions mathématiques intéressantes qui y sont rattachées : détermination des points d'inflexion en toute caractéristique ; sur un corps fini, existence d'une droite, voire d'une tangente, dont tous les points de contact avec la courbe sont rationnels. Pour ce dernier point, certains résultats annoncés dans [2] n'ont pas fait l'objet d'une publication. Il nous a semblé utile d'inclure les démonstrations dans l'appendice au chapitre 6.

5.1.1 Loi d'addition géométrique

Soit C une courbe de genre 3 non hyperelliptique sur un corps K, plongée canoniquement dans $\mathbb{P}^2$ comme une quartique plane lisse. On suppose qu'il existe une droite ℓ^∞ qui coupe la quartique en quatre points rationnels (distincts ou non) P_i^∞ et on pose $D^\infty = P_1^\infty + P_2^\infty + P_3^\infty$ la somme de trois d'entre eux. L'application de $\mathrm{Sym}^3 C \to \mathrm{Jac}\, C$ qui à un diviseur D^+ effectif de degré 3 associe (la classe) du diviseur $D^+ - D^\infty$ est surjective et génériquement injective. On représentera un élément de la jacobienne par D^+ et on cherche donc à calculer génériquement et efficacement le diviseur D^+ associé à $D = D_1 + D_2$ en fonction de D_1^+, D_2^+.

En utilisant le fait que pour une courbe plane C' de degré n on a $(C' \cdot C) \sim n\kappa$ où κ est le diviseur canonique de C puis en appliquant le théorème de Bézout, on obtient facilement l'algorithme d'addition suivant [2, Prop.1.1].

1. Soit E une cubique plane passant (avec multiplicité) par les points du support de D_1^+, D_2^+ et $P_1^\infty, P_2^\infty, P_4^\infty$. Le diviseur résiduel D_3^+ de l'intersection de C et E est de degré 3.
2. Soit Q la conique passant par D_3^+ et P_1^∞, P_2^∞. Le diviseur résiduel de l'intersection de Q et C est le diviseur D^+.

Le dessin ci-dessous représente la situation. On a noté

$$D_1^+ = P_1 + P_2 + P_3, D_2^+ = Q_1 + Q_2 + Q_3, D_3^+ = R_1 + R_2 + R_3 \text{ et } D^+ = K_1 + K_2 + K_3.$$

Remarque 5.1.1. Pour être efficace, on ne souhaite pas réaliser les opérations dans les extensions où sont définis les supports des diviseurs. On travaille donc avec leur représentation de Mumford (voir [Mum07, p.317], [CFA+06, p.306]). Notons que dans l'article

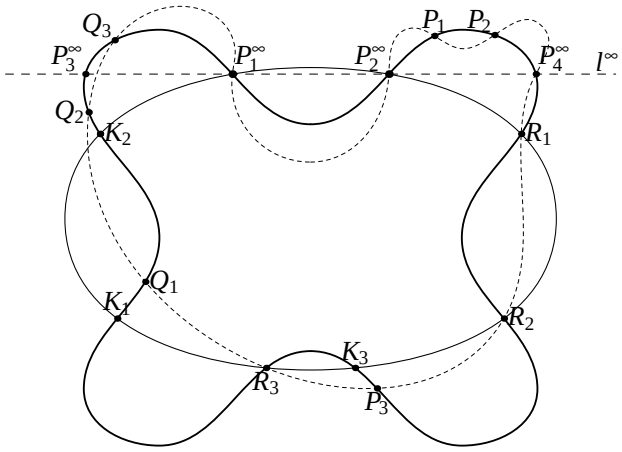


Figure 5.1 – Description de l'algorithme

on se restreint à des diviseurs "typiques" [2, Sec.3.1] pour limiter le nombre de cas à étudier.

On souhaite également, dans le cas des corps finis, optimiser le nombre d'opérations afin de rendre ces courbes compétitives avec les courbes de genre 1 ou 2. On cherche quelle est l'influence de la forme du diviseur $\ell^\infty \cdot C$ sur le modèle de C.

1. Cas générique : on peut écrire $C : y^3 + h_1(x)y^2 + h_2(x)y = f_4(x)$ avec $\deg(f_4) \leq 4$.
2. Cas $P_1^\infty = P_2^\infty$ (la droite ℓ^∞ est tangente en ce point) : $\deg(h_1) \leq 2$ et $\deg(h_2) \leq 3$.
3. Cas $P_1^\infty = P_2^\infty = P_4^\infty$ (le point est un *point d'inflexion*) : $\deg(h_1) \leq 2$ et $\deg(h_2) \leq 3$. Si de plus $\mathrm{car}(K) \neq 3$ on peut prendre $C : y^3 + h_2(x)y = f_4(x)$.
4. Cas $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$ (le point est un *point d'hyperinflexion*) : les quartiques lisses possédant un tel point forment une famille de codimension 1. Ce cas correspond aux courbes $C_{3,4}$ [2, Prop.2.1].
5. Si $\mathrm{car}\, K \neq 3$ on peut prendre $C : y^3 = f_4(x)$ (courbe de Picard) si et seulement si P_1^∞ est un point galoisien (en particulier c'est un point d'hyperinflexion) [2, Prop.2.2].

Rappelons qu'un point $P \in C(K)$ est dit *galoisien* si l'application $\phi_P : C \to |\kappa - P| = \mathbb{P}^1$, induite par le système linéaire $|\kappa - P|$ des droites passant par P, définit un revêtement géométrique galoisien de degré 3. On renvoie à la partie 6.1 pour plus de détails.

Bien évidemment, la morale de l'histoire est que plus la situation est particulière, plus on peut réduire le nombre de coefficients et moins les opérations d'addition sont coûteuses. Dans la section suivante, on verra jusqu'à quel point on peut satisfaire ces contraintes.

5.1.2 Etude de la condition de rationnalité sur les corps finis

Notre algorithme présuppose l'existence d'une droite ℓ^∞ coupant la quartique en quatre points rationnels. Dans le cas d'un corps quelconque (en particulier un corps de nombres), cette condition n'est bien sûr pas toujours réalisable. Cependant, c'est le cas sur les corps finis, lorsque le cardinal du corps est suffisamment grand.

Théorème 5.1.2 ([2, Th.2.1])**.** *Soit C une quartique plane lisse sur $k = \mathbb{F}_q$. Si $q \geq 127$, il existe toujours une droite coupant la quartique en quatre points rationnels.*

L'idée de la démonstration est d'utiliser le théorème de densité de Chebotarev pour les corps de fonctions (voir [KMS94]), afin d'estimer pour un point rationnel $P \in C(k)$ le nombre de diviseurs totalement décomposés du système linéaire $|\kappa - P|$. Un des termes de l'estimation est le nombre de points galoisiens sur $\bar{k}$. On montre que ce nombre est au plus 4 si $\operatorname{car} k \neq 3$ et 28 sinon. On renvoie à la partie 6.2 pour la démonstration complète.

On peut même demander que deux points soient identiques (c.-à-d. que ℓ^∞ soit tangente).

Théorème 5.1.3 ([2, Th.2.2])**.** *Soit C une quartique plane lisse sur $k = \mathbb{F}_q$ de caractéristique différente de 2. Si $q \geq 66^2 + 1$, il existe une tangente à C qui coupe la courbe en des points rationnels.*

Le principe de démonstration est complètement différent. Soit $T : C \to \operatorname{Sym}^2 C$ l'application qui à $P \in C$ associe $T_P(C) \cdot C - 2P$ où $T_P(C)$ est la droite tangente à C en P. L'application T s'appelle la *correspondance tangentielle* et on lui associe la courbe de correspondance définie sur k

$$X_C = \{(P, Q) \in C \times C \mid Q \in T(P)\}.$$

On souhaite montrer que X_C a toujours un point rationnel si q est assez grand. La courbe étant singulière, on utilise les résultats de [AP95]. Ces résultats s'appliquent lorsque la courbe est absolument irréductible. On vérifie que c'est le cas en montrant que la première projection $p_1 : X_C \to C$ est un morphisme de degré 2 qui se ramifie en un point $P_0 \in C(\bar{k})$ dont les antécédents par p_1 ne sont pas singuliers. Si $\operatorname{car} k \neq 2$, un tel point P_0 correspond à un point de bitangence qui n'est pas un point d'hyperinflexion. Un tel point existe toujours si $\operatorname{car} k \neq 3$ ou si la courbe n'est pas géométriquement isomorphe à $x^4 + y^4 + z^4 = 0$ (on traite ce cas à part). Enfin pour obtenir explicitement la borne, on montre que le genre arithmétique de X_C vaut 33. On renvoie à la partie 6.3 pour la démonstration complète.

Question : Peut-on éliminer l'hypothèse sur la caractéristique ?

Peut-on demander encore plus ? Quand $\operatorname{car} k > 3$, une quartique plane lisse a 24 points d'inflexion comptés avec multiplicité. Des arguments heuristiques, confirmés par des calculs, indiquent que la probabilité qu'une quartique lisse C sur $\mathbb{F}_q$ ait au moins un

point d'inflexion rationnel est d'environ 0.63 quand q tend vers l'infini [2, Conj.2.1]. Ceci semble encore vrai en caractéristique 2 et 3.

Question : Peut-on démontrer ces affirmations ?

Ce cas est suffisamment probable pour qu'il soit considéré dans nos applications. En pratique, on a besoin pour cela de déterminer les points d'inflexion en toute caractéristique. Or la méthode classique d'intersection avec la hessienne ne fonctionne plus en caractéristique 2 et 3. Nous proposons dans [2, Appendix] une méthode valide en toute caractéristique pour toute courbe plane. Ceci généralise le résultat de [Abh63] valide en toute caractéristique différente de 2. Nous avons découvert plus tard que ce résultat est aussi démontré dans [SV86, Th.0.1] par d'autres méthodes.

Enfin une quartique générique n'ayant pas de point d'hyperinflexion, on ne peut demander plus. Notons néanmoins que si car $k > 3$ et si la quartique a un point d'inflexion alors génériquement (dans cette famille), il est unique [Ver83] et donc rationnel.

5.2 Couplage rapide sur les courbes d'Edwards

Cette partie se rapporte à l'article [1'] avec Christophe Arène, Tanja Lange et Michael Naehrig.

Le domaine de la cryptographie à clé publique a récemment vu se développer un vif engouement pour deux nouvelles notions. D'un côté, la notion de couplage qui permet par exemple l'échange tri-partie, la signature basée sur l'identité ou des signatures courtes (voir [CFA+06, Chap.24]). Dans le cas de la cryptographie elliptique (voire hyperelliptique), cela se traduit par l'utilisation de différentes notions de couplages algébriques : couplage de Weil, Tate, eta, Ate, R-ate etc. et l'optimisation de leur calcul. De l'autre, les *courbes d'Edwards* : ces courbes, introduites en cryptographie par Bernstein et Lange [BL07], sont des quartiques de la forme

$$E_d : ax^2 + y^2 = 1 + dx^2y^2.$$

On suppose ici la caractéristique du corps différente de 2 (voir [BLRF08] pour un modèle dans le cas contraire). Leurs deux points à l'infini sont singuliers et elles sont birationnellement équivalentes à des courbes elliptiques. Elles possèdent une structure de groupe qui est intéressante à plusieurs titres :

1. La loi d'addition est *unifiée*, c.-à-d. elle peut s'effectuer par une formule unique que ce soit pour l'addition de deux points génériques ou pour le doublement d'un point générique. Elle est même *fortement unifiée*, c.-à-d. l'addition du neutre, ici $(0, 1)$, avec un point générique se fait par la même formule.
2. Lorsque d n'est pas un carré dans le corps, la loi d'addition unifiée est *arithmétiquement complète*, c.-à-d. qu'on peut additionner entre eux tous les points rationnels

affines avec cette unique formule et ceux-ci forment un groupe pour cette loi. On reviendra sur ce sujet dans la section 5.2.3.

3. Sur les corps finis, ces opérations peuvent être rendues très rapides (certes au prix de la perte de la propriété d'être unifiée) : l'addition coûte $10\boldsymbol{m} + 1\boldsymbol{s} + 1\boldsymbol{d}$ et le doublement $3\boldsymbol{m} + 4\boldsymbol{s}$. On a noté $\boldsymbol{m}$ (resp. $\boldsymbol{s}$, $\boldsymbol{d}$) le coût d'une multiplication (resp. d'un carré, d'une multiplication par la constante d) dans le corps.

Les deux premières propriétés ont un intérêt en cryptographie puisqu'elles empêchent les *attaques par canaux cachés* [CFA+06, Chap.28], qui profitent des variations (de consommation d'énergie, de temps d'exécution) entre l'addition et le doublement ou de la gestion des exceptions dans un système embarqué pour obtenir des informations sur le secret.

Notre article se situe à la confluence des notions de couplage et des courbes d'Edwards. Nous donnons ci-dessous la description géométrique de la loi de groupe pour ces courbes et son utilisation dans l'algorithme de Miller pour le calcul du couplage.

5.2.1 Loi d'addition géométrique

Lorsque Edwards dans [Edw07] a introduit le modèle qui porte son nom, il a donné plusieurs démonstrations de la loi de groupe (par exemple en utilisant les fonctions thêta) mais, curieusement, aucune démonstration géométrique alors que dans le cas des équations de Weierstrass, la description géométrique est souvent la première donnée. Ceci peut pourtant se faire de manière assez simple, par analogie d'ailleurs avec le cas des quartiques lisses étudiées dans la partie 5.1.

Soit K un corps de caractéristique différente de 2. On appelle *courbe d'Edwards tordue* sur K la courbe de modèle affine

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2, \quad a, d \in K^*, a \neq d.$$

On supposera de plus que ad n'est pas un carré dans K (afin que la loi d'addition ci-dessous soit arithmétiquement complète). Ce modèle, un peu plus général que celui d'Edwards (où $a = 1$), a été introduit dans [BBJ+08] pour obtenir une famille de courbes stable par torsion quadratique. La loi d'addition sur les points affines est donnée par

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

On note $\mathcal{O} = (0, 1)$ l'élément neutre pour la loi, l'inverse étant $(x_1, y_1) \mapsto (-x_1, y_1)$. Le point $\mathcal{O}' = (0, -1)$ est un point d'ordre 2. Les points à l'infini $\Omega_1 = (1 : 0 : 0)$ et $\Omega_2 = (0 : 1 : 0)$ sont les seuls points singuliers.

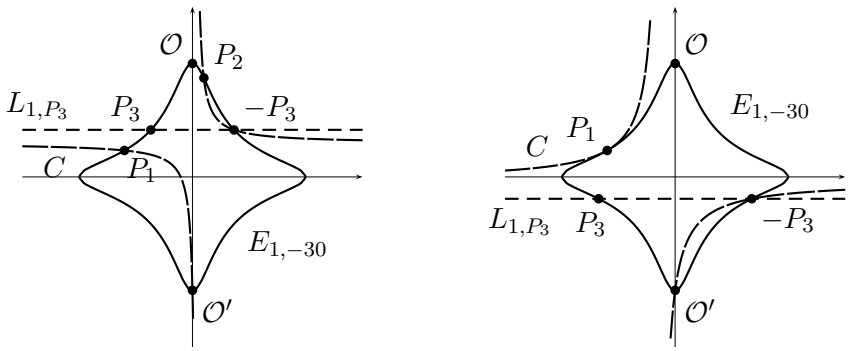
Théorème 5.2.1 ([1', Th.2],[Arè08])**.** *Soit $P_1, P_2 \in E_{a,d}(K)$. Le point $P_3 = P_1 + P_2$ est obtenu géométriquement comme suit*

1. *Soit C l'unique conique passant par $\Omega_1, \Omega_2, \mathcal{O}', P_1$ et P_2 (avec multiplicité le cas échéant) ;*
2. *Les points Ω_i étant singuliers, la conique C recoupe la quartique $E_{a,d}$ en un unique "huitième" point $P' = -P_3$;*
3. *Le symétrique de P' par rapport à l'axe des ordonnées est le point P_3.*

Illustrons ces constructions sur les dessins suivants. Soient

$$E_{1,-30} : x^2 + y^2 = 1 - 30x^2y^2$$

sur $\mathbb{R}$, $P_1 = (x_1, y_1)$ avec $x_1 = -0.6$ et $P_2 = (x_2, y_2)$ avec $x_2 = 0.1$. Le dessin 5.2(a) montre la loi d'addition de P_1 et P_2, et le dessin 5.2(b) montre le doublement du point P_1.



(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$, $P_3 = P_1 + P_2$ (b) $P_1 = P_2 \neq \mathcal{O}'$, $P_3 = 2P_1$

Figure 5.2 – Interprétation géométrique de la loi de groupe de $x^2 + y^2 = 1 - 30x^2y^2$ sur $\mathbb{R}$.

5.2.2 Utilisation avec le couplage de Tate

Soit $E/\mathbb{F}_q$ une courbe elliptique d'élément neutre $\mathcal{O}$ et $r|\#E(\mathbb{F}_q)$ un nombre premier. On suppose de plus que E a un *degré de plongement* $s > 1$ par rapport à r, c.-à-d. s est le plus petit entier tel que $q^s \equiv 1 \pmod{r}$. Soit $P \in E(\mathbb{F}_q)[r]$ et soit $f_P \in \mathbb{F}_q(E)$ la fonction définie à un scalaire multiplicatif près par $\mathrm{div}(f_P) = r(P) - r(\mathcal{O})$. Soit $\mu_r \subset \mathbb{F}_{q^s}^*$ le groupe des racines r-ième de l'unité. Le *couplage de Tate* (réduit) est l'application bilinéaire non dégénérée

$$T_r : E[r](\mathbb{F}_q) \times E(\mathbb{F}_{q^s})/rE(\mathbb{F}_{q^s}) \to \mu_r, \quad (P, Q) \mapsto f_P(Q)^{(q^s-1)/r}.$$

L'intérêt de ce couplage en cryptographie est qu'il peut se calculer très rapidement de manière itérative grâce à l'algorithme de Miller [Mil04]. Soit $r = (r_{l-1}, \ldots, r_1, r_0)_2$ l'écriture en base 2 de r et soit $g_{R,P} \in \mathbb{F}_q(E)$ la fonction d'addition sur E, c.-à-d. le diviseur $\mathrm{div}(g_{R,P}) = (R) + (P) - (R + P) - \mathcal{O}$. L'algorithme de Miller commence avec $R = P$ et $f = 1$ et calcule

1. for $i = l - 2$ to 0 do
   (a) $f \leftarrow f^2 \cdot g_{R,R}(Q),\ R \leftarrow 2R$ //doublement
   (b) if $r_i = 1$ then $f \leftarrow f \cdot g_{R,P}(Q),\ R \leftarrow R + P$ //addition
2. $f_P \leftarrow f^{(q^s-1)/r}$.

Dans le cas du modèle de Weierstrass on utilise pour l'expression de $g_{R,P}$ les coordonnées jacobiennes (étendues) (voir `http://www.hyperelliptic.org/EFD`). Dans l'article, on montre que le coût pour le calcul du couplage de Tate dans ce cas peut être diminué par rapport à ceux de la littérature [1', Sec.3].
Dans le cas du modèle d'Edwards, grâce à la loi de groupe géométrique, on a $g_{R,P} = \frac{\phi}{l_1 l_2}$ où ϕ est une équation de la conique passant par $P, R, \Omega_1, \Omega_2, \mathcal{O}'$, l_1 une équation de la droite $\overline{(R+P)\Omega_2}$ et l_2 une équation de la droite $\overline{\mathcal{O}\mathcal{O}'}$. Une succession d'astuces de calcul permet alors d'améliorer nettement les résultats de [IJ08] pour le calcul du couplage. On renvoie à [1', Sec.4] pour des comparaisons plus détaillées.

Pour les applications cryptographiques, on cherche des courbes sur $\mathbb{F}_p$ dont l'ordre du groupe des points rationnels est divisible par un grand nombre premier r et avec un degré de plongement s relativement petit ($4 \leq s \leq 22$). Dans le cas des courbes d'Edwards, il y a une dernière contrainte : une courbe elliptique sur un corps fini est birationnellement équivalente à une courbe d'Edwards si et seulement si elle a un point de 4-torsion rationnel. On applique la stratégie suivante. En utilisant les constructions CM pour certaines familles de paramètres de [GP08] et [FST06], on obtient des courbes elliptiques $E/\mathbb{F}_p$ avec les propriétés ci-dessus et telles que $4|\#E(\mathbb{F}_p)$. Par exemple dans le cas $s = 6$, les paramètres possibles sont les suivants

$p = q(X)$	$t = t(X)$
$16X^2 + 10X + 5$	$2X + 2$
$112X^2 + 54X + 7$	$14X + 4$
$112X^2 + 86X + 17$	$14X + 6$
$208X^2 + 30X + 1$	$-26X - 2$
$208X^2 + 126X + 19$	$-26X - 8$

où t est la trace de la courbe E que l'on souhaite construire. On cherche donc $l \in \mathbb{Z}$ tel que

1. $q(l)$ est un nombre premier avec $t(l)^2 - 4q(l) = -dy^2$ et le discriminant d assez petit pour pouvoir construire la courbe par CM ;
2. $q(l) + 1 - t(l)$ est divisible par un grand nombre premier.

Après cela, par une suite de 2-isogénies, on montre qu'on peut toujours transformer E en une courbe E' avec un point rationnel de 4-torsion [Mor09] (c'est une application de la théorie des volcans d'isogénies). Il suffit alors de prendre le modèle d'Edwards associé à E'. On renvoie à [1', Sec.8] pour des exemples de taille cryptographique.

5.2.3 Autour des modèles d'Edwards

La "découverte" du modèle d'Edwards et de ses propriétés induit tout naturellement des questions autour de ses analogues : peut-on trouver pour d'autres modèles de courbes elliptiques une loi unifiée complète (en particulier en caractéristique 2) ? Pour les (jacobiennes des) courbes de genre 2 ? Et ce de telle manière que la loi d'addition soit efficace ? C'est le sujet de thèse de mon étudiant Christophe Arène, en co-direction avec David Kohel.
Un des premiers objectifs sera d'établir un cadre théorique adéquat. En accord avec Kohel, on distingue trois notions de complétude. Tout d'abord la complétude géométrique. Soit A une variété abélienne de dimension $g > 0$ sur un corps algébriquement clos K. On dira qu'un ensemble S de lois d'addition sur A est *géométriquement complet* si, pour tout couple de points de $A(K)$, il existe une loi d'addition dans S qui permette d'additionner ces deux points. L'article [BL95] montre que dans le cas du modèle de Weierstrass deux lois d'addition au moins sont nécessaires pour obtenir la complétude géométrique et donne une telle paire explicitement (les expressions sont très volumineuses). L'article [LR85] traite du cas des variétés abéliennes de dimension quelconque mais ne semble pas donner de résultat sur le cardinal minimal de S. On pourra raisonnablement commencer par montrer que $\#S > g$.
Un deuxième problème plus subtil est celui de la complétude arithmétique sur un corps K quelconque. Soit A une variété abélienne sur K. Un ensemble de lois d'addition S sur A est dit *arithmétiquement complet* s'il existe un ouvert U/K de A tel que $U(K) = A(K)$ et, pour tout couple de points rationnels, il existe une loi dans S permettant de les additionner. Pour le modèle d'Edwards E_d avec d qui n'est pas un carré dans K, cette propriété est obtenue avec $\#S = 1$. Peut-on retrouver ce résultat en genre supérieur ? Parallèlement à une analyse théorique du problème, on pourra essayer différentes généralisations naturelles des courbes d'Edwards en genre 2, telles que les quartiques avec un seul point singulier.
La loi d'addition pour E_d sur un corps fini k vérifie une propriété encore plus forte, qu'on appellera *complétude exceptionnelle*, par référence aux fonctions exceptionnelles. Celle-ci signifie que la complétude arithmétique pour S est valable pour une infinité d'extensions de k (dans le cas d'Edwards, les extensions non quadratiques). Cette propriété est évidemment la plus intéressante pour les applications cryptographiques.

5.3 Applications de distorsion

Dans cette partie j'expose les résultats de [3] avec Steven D. Galbraith, Jordi Pujolàs et Benjamin Smith.

Comme nous l'avons dit dans la partie 5.2, la notion de couplage est un concept important en cryptographie à clé publique. En particulier, si C est une courbe (projective, lisse, absolument irréductible) sur un corps fini $k = \mathbb{F}_q$, r un premier divisant

$\#(\mathrm{Jac}\, C)(k)$, on peut, par exemple, considérer le couplage de Weil

$$e_r : (\mathrm{Jac}\, C)[r](\bar{k}) \times (\mathrm{Jac}\, C)[r](\bar{k}) \to \mu_r \subset \mathbb{F}_{q^s}$$

où s est le degré de plongement relatif à r. Un tel couplage est bilinéaire et non dégénéré. Pour qu'il soit pertinent en cryptographie, il faut choisir $D_1, D_2 \in (\mathrm{Jac}\, C)[r](\bar{k})$ tels que $e_r(D_1, D_2) \neq 1$. Or, si pour des raisons d'efficacité, $D_1, D_2 \in (\mathrm{Jac}\, C)[r](k)$ et que $r||\#(\mathrm{Jac}\, C)(k)$ (c'est le cas dans les applications) alors $D_2 = aD_1$ pour $a \in \mathbb{Z}$ et le couplage est trivial. D'où la définition suivante.

Définition 5.3.1. Une *application de distorsion* pour $D_1, D_2 \in (\mathrm{Jac}\, C)[r](\bar{k}) \setminus \{0\}$ est un endomorphisme $\psi \in \mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$ tel que $e_r(D_1, \psi(D_2)) \neq 1$.

La notion a été introduite par [Ver01] dans le cas des courbes elliptiques et un algorithme pour les courbes elliptiques supersingulières a été donné dans [GR04]. Dans notre article, nous considérons le cas des courbes de genre 2 supersingulières. Dans ce cas, l'existence des applications de distorsion est assurée pour tout couple de diviseurs.

Théorème 5.3.2 ([3, Th.2.1])**.** *Soit A une variété abélienne supersingulière de dimension $g \geq 1$ sur k et soit r un premier différent de la caractéristique p de k. Pour tout couple de points $(D_1, D_2) \in A[r](\bar{k}) \setminus \{0\}$, il existe une application de distorsion.*

Étant donnés A et r, on dira qu'un ensemble fini S d'applications de distorsion est *complet* si pour tout couple $(D_1, D_2) \in A[r](\bar{k}) \setminus \{0\}$ il existe une application de distorsion pour D_1, D_2 dans S. On souhaite évidemment que $\#S$ soit le plus petit possible et que les éléments de S soient faciles à calculer.

Le cas supersingulier est donc le cadre naturel d'existence d'un ensemble complet d'applications de distorsion (on peut montrer qu'un tel ensemble n'existe pas toujours dans le cas ordinaire). Pour les courbes supersingulières, le degré de plongement s est borné par une constante ne dépendant que du genre (voir [Gal01] et [RS02]). Par exemple en genre 2, on a les possibilités suivantes lorsque $q = p$ (ou une puissance impaire)

p	degrés de plongement s possibles
2	$\{1, 3, 6, 12\}$
3	$\{1, 3, 4\}$
5	$\{1, 3, 4, 5, 6\}$
≥ 7	$\{1, 3, 4, 6\}$

Dans la suite, on exhibe pour les degrés de plongement les plus intéressants (c.-à-d. $s \geq 4$) des modèles de courbes $C/\mathbb{F}_p$ et un ensemble complet d'applications de distorsion pour r assez grand. Pour ce faire, on donne dans chacun des cas ci-dessus des générateurs de $\mathrm{End}^0_{\bar{k}}(\mathrm{Jac}\, C) = \mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C) \otimes \mathbb{Q}$ induits soit par l'application de Frobenius π soit par des $\bar{k}$-automorphismes de la courbe. Dans la suite si $\alpha_i \in \mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$, on note $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ le sous-anneau de $\mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$ engendré par les α_i et de même $\mathbb{Q}[\alpha_1, \ldots, \alpha_n] = \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \otimes \mathbb{Q}$ la $\mathbb{Q}$-sous-algèbre de $\mathrm{End}^0_{\bar{k}}(\mathrm{Jac}\, C)$.

5.3.1 Cas $s = 4$

On commence par donner deux résultats généraux. Soient p un premier, $k = \mathbb{F}_p$ et C/k une courbe de genre $g \geq 1$ telle que $\mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$ contienne un élément α qui engendre un corps CM, $F \subset \mathrm{End}^0_{\bar{k}}(\mathrm{Jac}\, C)$ de degré $2g$ sur $\mathbb{Q}$. Soit $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ l'automorphisme de Frobenius. On suppose que le corps de définition de α est $\mathbb{F}_{p^{2g}}$ et que α commute avec α^σ. Soit enfin $\pi \in \mathrm{End}(\mathrm{Jac}\, C)$ l'endomorphisme de Frobenius sur k.

Proposition 5.3.3 ([3, Prop.4.1, Cor.4.4])**.** *Sous ces hypothèses,* $\mathrm{Jac}\, C$ *est supersingulière et*

$$\mathrm{End}^0_{\bar{k}}(\mathrm{Jac}\, C) = \mathbb{Q}[\pi, \alpha] = \left\{ \sum_{0 \leq i,j \leq 2g-1} \lambda_{i,j} \pi^i \alpha^j,\ \lambda_{i,j} \in \mathbb{Q} \right\}.$$

Soit $r > 1$ premier à l'indice de $\mathbb{Z}[\pi, \alpha]$ dans $\mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$. L'ensemble

$$\{\pi^i \alpha^j,\ 0 \leq i, j \leq 2g-1\}$$

est un ensemble complet d'applications de distorsion pour $\mathrm{Jac}\, C$ *et r.*

Nous souhaitons aussi avoir un contrôle sur le degré de plongement. On l'obtient par une application de la théorie CM [Lan83, §6].

Proposition 5.3.4 ([3, Cor.4.6])**.** *Soit $\tilde{C}/\mathbb{Q}$ une courbe de genre $g \geq 1$ telle que* $\mathrm{Jac}\, \tilde{C}$ *soit absolument simple et* $\mathrm{End}^0_{\mathbb{Q}}(\mathrm{Jac}\, \tilde{C})$ *contienne un corps CM galoisien F de degré $2g$. Si p est un premier inerte de F alors* $\mathrm{Jac}\, \tilde{C}$ *a bonne réduction en p et le polynôme de Weil de la réduction sur $\mathbb{F}_p$ est $T^{2g} + p^g$. En particulier le degré de plongement est $2g/t$ avec t un diviseur impair de g.*

Remarque 5.3.5. Bien que le résultat soit "local", on a besoin de commencer avec une courbe CM sur $\mathbb{Q}$, sinon le résultat peut être faux (voir [3, Rem.4.7]).

Les résultats précédents peuvent s'appliquer pour les courbes sur $\mathbb{F}_p$ de la forme $y^2 = x^{2g+1} + A$ avec $2g+1$ premier, p primitif modulo $2g+1$ et $A \in \mathbb{F}_p^*$. À la suite de notre article, Takashima dans [Tak08] a montré que pour $A = 1$ et $r > 5$, l'hypothèse "r premier à l'indice de $\mathbb{Z}[\pi, \alpha]$ dans $\mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$" était satisfaite. Dans le cas du genre 2 en particulier on obtient le résultat suivant.

Proposition 5.3.6. *Soit $p \equiv 2, 3 \pmod 5$ et $C/\mathbb{F}_p : y^2 = x^5 + 1$. La courbe C est supersingulière et son degré de plongement est 4. Soit $\alpha : (x, y) \mapsto (\zeta_5 x, y)$, avec ζ_5 une racine primitive cinquième de l'unité, un $\bar{k}$-automorphisme de C. Pour $r > 5$, l'ensemble*

$$\{\pi^i \alpha^j,\ 0 \leq i, j \leq 3\}$$

est un ensemble complet d'applications de distorsion pour les points de r-torsion non triviaux de $(\mathrm{Jac}\, C)[r](\bar{k})$.

5.3.2 Cas $s = 5$ et $s = 6$

Les courbes que l'on considère dans ces deux cas sont des tordues de la courbe $C : y^2 = x^6 + 1$.

1. Dans le cas $s = 5$, il s'agit des courbes $y^2 = x^5 - x + b$ avec $b = \pm 1$ sur $\mathbb{F}_{5^m}$ tel que $\mathrm{pgcd}(m, 10) = 1$ [DL03].
2. Dans le cas $s = 6$, seule l'existence de ces courbes était connue grâce aux résultats de [7]. Nous présentons une construction algorithmique dans [3, Th..5.6] et dans [CN07, Tab.9, ligne.5,6] on peut trouver des modèles.

Soit E la courbe elliptique $y^2 = x^3 + 1$. En utilisant la $(2, 2)$-isogénie explicite entre $\mathrm{Jac}\, C$ et $E \times E$, on peut démontrer que π (l'endomorphisme de Frobenius), $\chi : (x, y) \mapsto (1/x, y/x^3)$ et $\rho_6 : (x, y) \mapsto (\zeta_6 x, y)$ avec ζ_6 une racine sixième de l'unité, engendrent un ordre dans $\mathrm{End}_{\bar{k}}(\mathrm{Jac}\, C)$ d'indice divisant $2^8 3^4$. En utilisant les isomorphismes explicites vers les tordues, on importe ces endomorphismes et on obtient ainsi un système complet d'applications de distorsion explicites sous l'hypothèse que $r > 3$ [3, Sec.5.2,5.3].

5.3.3 Cas $s = 12$

Soit m un entier tel que $m \equiv \pm 1 \pmod 6$. On considère les courbes

$$C : y^2 + y = x^5 + x^3 + b$$

sur $k = \mathbb{F}_{2^m}$ avec $b = 0, 1$. Elles ont été étudiées dans [vdGvdV92b] et [vdGvdV92a] pour leurs applications en théorie des codes. Soit

$$\sigma_\omega : (x, y) \longmapsto (x + \omega, y + s_2 x^2 + s_1 x + s_0)$$

le $\bar{k}$-automorphisme de C avec ω une racine de

$$\begin{aligned} &T^{16} + T^8 + T^2 + T \\ &= (T^6 + T^5 + T^3 + T^2 + 1)(T^3 + T^2 + 1)(T^3 + T + 1)(T^2 + T + 1)(T + 1)T, \end{aligned}$$

$s_2 = \omega^8 + \omega^4$, $s_1 = \omega^4 + \omega^2$ et s_0 une racine de $y^2 + y = \omega^5 + \omega^3$. Soit $\tau \in \mathbb{F}_{2^6}$ une racine de $T^6 + T^5 + T^3 + T^2 + 1$, $\chi = \tau^4 + \tau^2$ et $\theta = \chi + \tau$. On montre alors que $\mathrm{End}^0_{\bar{k}}(\mathrm{Jac}\, C) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$ [3, Prop.6.1]. Un résultat plus récent de [Tak08, Th.10] établit que si $r > 19$, l'ensemble $\{\pi^i, \pi^j \sigma_\theta, \pi^s \sigma_\tau, \pi^t \sigma_\chi,\ 0 \le i, j, s, t \le 3\}$ est un ensemble complet d'applications de distorsion pour r et $\mathrm{Jac}\, C$.

5.4 Méthode CM 2-adique pour les courbes de genre 2

Cette partie expose les résultats de [4] avec Pierrick Gaudry, Thomas Houtmann, David Kohel et Annegret Weng.

Le variétés abéliennes (essentiellement en dimension $g = 1$ ou 2) sur un corps fini k jouent un rôle central en cryptographie à clé publique depuis leur introduction par Koblitz et Miller en 1985. Leur groupe des points rationnels sert en effet de base pour des

protocoles utilisant le problème du logarithme discret et plus récemment les couplages comme on l'a vu dans les parties 5.2 et 5.3. Leur avantage principal sur les systèmes classiques basés sur la factorisation ou le problème du logarithme discret dans $\mathbb{F}_q^*$ est qu'on ne connaît pas pour l'heure d'attaque sous-exponentielle dans le cas général. Toutefois, pour résister aux attaques génériques sur tout groupe fini, celui-ci doit avoir un grand ordre premier ou tout au moins être divisible par un grand facteur premier (et donc q doit être grand). Deux types de stratégie existent pour parvenir à cela (voir [CL06] et `http://iml.univ-mrs.fr/~ritzenth/slides/expo_C2.pdf` pour un survol).

- on peut prendre des courbes C au hasard sur $\mathbb{F}_q$ et calculer rapidement $\#(\mathrm{Jac}\, C)(k)$ jusqu'à obtenir la propriété désirée. Les algorithmes se répartissent en deux catégories :
  - Lorsque p est petit (et n grand), un grand nombre d'algorithmes efficaces existent : relèvement canonique (Satoh, AGM, etc.), méthodes cohomologiques (de Monsky-Washnitzer, de Dwork-Reich, rigide, etc.) ou déformation (Lauder et Wan, Hubrechts). Par exemple pour $p = 2$, le record actuel, obtenu par l'AGM, est sur $\mathbb{F}_{2^{100002}}$ en genre 1 et sur $\mathbb{F}_{2^{32770}}$ en genre 2 (Lercier-Lubicz 2002-2003).
  - Lorsque p est grand (et n petit, ici 1) et $g = 1$, la seule méthode connue est la méthode ℓ-adique due à Schoof. Les améliorations d'Atkin et d'Elkies (voir [Sch95]) ont donné naissance à l'algorithme SEA et ont permis de ramener la complexité de $\mathcal{O}((\log p)^{2+3\mu})$ à $\mathcal{O}((\log p)^{2+\mu})$, où $1 \leq \mu \leq 2$ est l'exposant de la complexité de la multiplication dans $\mathbb{F}_p$. Le record actuel est $p = 10^{2499} + 7131$ (Enge-Morain 2006). En genre 2, la situation est moins bonne et on peine à atteindre les tailles cryptographiques (voir tout de même les résultats récents de Gaudry et Schost `http://www.loria.fr/~gaudry/record127/` pour $p = 2^{127} - 1$). Pour y remédier, nous commençons un projet ANR en collaboration avec Rennes et Nancy sur ce sujet (voir `http://chic.gforge.inria.fr/`).
- inversement on peut construire une courbe fixe C sur un corps de nombres et faire varier le premier p de réduction jusqu'à ce que le groupe des points rationnels de $\mathrm{Jac}\, C \pmod p$ ait la propriété souhaitée. Pour que ceci soit efficace, on munit la courbe C d'une structure supplémentaire avec laquelle le calcul de l'ordre du groupe est aisé.

La structure la plus étudiée est celle dite de *multiplication complexe* (CM). On considère ici la notion dans son sens strict : une courbe C de genre g sera CM si $\mathrm{End}^0(\mathrm{Jac}\, C)$ est un corps K CM (c.-à-d. une extension imaginaire quadratique d'un corps totalement réel K^+) de degré $2g$. La première méthode inventée pour construire de telles courbes est la méthode complexe (voir section 5.4.1). Nous proposons ici une alternative à cette méthode dans le cas du genre 2. L'idée à la base de l'article est simple et s'inspire des travaux de [CH02] et [BS04] en genre 1 : sur les corps de nombres les courbes CM sont rares ; au contraire sur un corps fini, elles sont fréquentes puisqu'il suffit par exemple que la courbe soit ordinaire et sa jacobienne absolument irréductible. Il suffit donc de relever "canoniquement" une telle courbe pour obtenir une courbe CM. Nous expliquons comment réaliser cette opération dans la section 5.4.2. Si les méthodes CM sont bien comprises en genre 1 (avec des constructions quasi-optimales [BBEL08]), un certain nombre de questions demeurent en genre 2, voire 3. Dans la section 5.4.3 nous décrivons

quelques sujets d'étude.

5.4.1 Principe de la méthode complexe en genre 2

Les références pour la théorie en genre 2 sont [Spa94], [vW99] et [Wen03].
On se place dans le cas où $g = 2$ et le corps $K/\mathbb{Q}$ est une extension CM de degré 4 d'anneau des entiers $\mathcal{O}_K$. À un tel corps, on associe un *type* donné par une paire de plongements non conjugués $\Phi = \{\phi_1, \phi_2\}$ de K dans $\mathbb{C}$. Si I est un idéal de $\mathcal{O}_K$, on considère $\Phi(I) = \{(\phi_1(\alpha), \phi_2(\alpha)) \subset \mathbb{C}^2, \alpha \in I\}$. C'est un réseau de $\mathbb{C}^2$ et on montre que $\mathbb{C}^2/\Phi(I)$ est une variété abélienne A telle que $K \subset \mathrm{End}^0(A)$. On fait ici plusieurs simplifications théoriques commodes et restrictions d'ordre algorithmique :

1. On suppose que K est *primitif*, c.-à-d. dans le cas $g = 2$, que K est cyclique ou n'est pas galoisien. Dans ce cas A est absolument simple, ce qui est une bonne condition pour la cryptographie, et $K \simeq \mathrm{End}^0(A)$. On supposera également que $K \neq \mathbb{Q}(\zeta_5)$.

2. On suppose que le nombre de classes de K^+, noté h_{K^+}, est égal à 1. Les arguments heuristiques de Cohen-Lenstra impliquent que $h_{K^+} = 1$ avec une densité supérieure à 3/4. Cette condition n'est donc pas très restrictive. Dans ce cas, A a une polarisation principale. Puisque A est absolument simple c'est la jacobienne d'une courbe C de genre 2 [OU73].

3. On suppose que $\mathrm{End}(A) \simeq \mathcal{O}_K$.

On dira sous ces hypothèses que C (ou A) est à *multiplication complexe par* $\mathcal{O}_K$.

Schématiquement, on procède comme suit (voir [CFA+06, 18.2] et [Str09]).

1. On construit l'ensemble T des classes d'isomophisme de surfaces abéliennes principalement polarisées avec multiplication complexe par $\mathcal{O}_K$. Si K est cyclique (resp. n'est pas galoisien) alors $\#T = h_K$ (resp. $\#T = 2h_K$) où h_K est le nombre de classes de K.

2. On représente chaque élément de T par une matrice $\tau_i \in \mathbb{H}_2$ telle que $A_i(\mathbb{C}) \simeq A_{\tau_i}$. Pour chaque A_i, on calcule les ThetaNullwerte, puis grâce aux formules de Rosenhain on trouve une équation de la courbe et les invariants absolus j_1, j_2, j_3 (voir paragraphe 2.2.1). On peut combiner ces deux étapes pour obtenir directement les invariants. Donnons ici les formules de [Str09, Sec.8.1]. Soient S_2 l'ensemble des thêta caractéristiques pairs (voir définition 4.2.1) et

$$L = \{C \subset S_2,\ \#C = 6 \text{ et } \sum_{c \in C} c \in \mathbb{Z}^2 \oplus \mathbb{Z}^2\}.$$

Soient

$$\begin{aligned} h_4 &= \sum_{c\in S_2} \theta[c]^8, \\ h_{10} &= \prod_{c\in S_2} \theta[c]^2, \\ h_{12} &= \sum_{C\in L} \prod_{c\in C} \theta[c]^4, \\ h_{16} &= \sum_{C\in L, d\in S_2\setminus C} \theta[d]^8 \prod_{c\in C} \theta[c]^4. \end{aligned}$$

Alors $I_2 = h_{12}/h_{10}$, $I_4 = h_4$, $I_6 = h_{16}/h_{10}$ et $I_{10} = h_{10}$.

3. On calcule ensuite les *polynômes de classes d'Igusa*

$$H_m(X) = \prod_T (X - j_m) \in \mathbb{Q}[X]$$

pour $m = 1, 2, 3$. Contrairement au cas $g = 1$, les coefficients de ces polynômes ne sont pas entiers.

4. On cherche les premiers p qui sont non ramifiés dans K, qui ne divisent pas les dénominateurs des coefficients des H_m, et pour lesquels l'équation aux normes $N_{K/K^+}(\pi) = p$ a des solutions (2 dans le cas cyclique, 2 ou 4 dans le cas non-galoisien). Soit f_π le polynôme minimal de π. On cherche si $f_\pi(1)$ est premier ou possède un grand facteur premier. Si ce n'est pas le cas, on change de p.
5. On réduit les polynômes de classes modulo p et on considère $(j_1, j_2, j_3) \in \mathbb{F}_p^3$ un triplet d'invariants absolus racines des $H_m \pmod p$.
6. En utilisant les algorithmes de reconstruction (voir section 2.5) on construit une courbe $\tilde{C}/\mathbb{F}_p$ telle que $\#(\mathrm{Jac}\,\tilde{C})(\mathbb{F}_p) = f_\pi(1)$.

Remarque 5.4.1. Certaines propriétés de $\mathrm{Jac}\,\tilde{C}$ (simplicité, p-rang) peuvent se lire sur la décomposition de p dans la clôture galoisienne L de $K/\mathbb{Q}$ (voir [Gor97] pour les cas où p est non ramifié dans L, [4, Th.3.5] dans sa version Arxiv ou [OMNS08] pour le cas général).

Notre méthode emprunte à la méthode complexe les étapes (4),(5) et (6) ci-dessus. Nous allons voir par quoi remplacer les trois premières étapes.

5.4.2 Principe de la méthode p-adique

Soit $\tilde{C}/k$ une courbe de genre 2 ordinaire dont la jacobienne est absolument simple. Sous ces hypothèses, $\mathrm{End}^0(\mathrm{Jac}\,\tilde{C})$ est un corps K CM [Tat66, Th.2.c)]. On suppose que K et $\tilde{C}$ vérifient les hypothèses de la section précédente, en particulier l'égalité $\mathrm{End}(\mathrm{Jac}\,\tilde{C}) = \mathcal{O}_K$. On note également $\mathbb{Q}_q$ l'unique extension non-ramifiée de $\mathbb{Q}_p$ de degré n et $\mathbb{Z}_q$ son anneau des entiers. La théorie du relèvement canonique [LST64] montre qu'il existe à isomorphisme près un unique schéma abélien principalement polarisé $\mathcal{A}$ sur

$\mathbb{Z}_q$ tel que la fibre spéciale de $\mathcal{A}$ soit $\operatorname{Jac} C$ et tel que sa fibre générique, notée $A/\mathbb{Q}_q$, vérifie $\operatorname{End}(A) = \operatorname{End}(\operatorname{Jac} C)$. Les hypothèses sur C montrent que A est elle-aussi à multiplication complexe par $\mathcal{O}_K$. La variété A est de ce fait définie sur un corps de nombres K'. Puisque $\operatorname{Jac} C$ est absolument irréductible, A l'est également et c'est donc la jacobienne d'une courbe C/K' de genre 2.

Dans l'article, on suppose que $p = 2$. On relève la courbe $\tilde{C}$ en une courbe $\mathcal{C}$ sur $\mathbb{Z}_q$ de manière arbitraire (dans la pratique on choisit tout de même avec soin le modèle pour que les calculs à venir restent dans $\mathbb{Q}_q$, voir [4, Rem.3]). Le relèvement canonique peut alors être approché grâce à la méthode AGM de Mestre [LL06],[6']. Il en existe deux variantes. Soit on travaille au niveau de la courbe $\mathcal{C}$ et on applique une suite d'isogénies de Richelot [4, Sec.4.1]. Rappelons que les isogénies de Richelot définissent une correspondance explicite entre deux courbes de genre 2 de telle sorte que leur jacobienne soit $(2,2)$-isogène. Soit on utilise une suite de moyennes de Borchard [Mes91b] qui fournissent des formules de duplication pour les ThetaNullwerte (algébriques) associées à $\operatorname{Jac}\mathcal{C}$ (voir Th. 4.2.2). Dans les deux cas, les résultats de [Car04] montrent la convergence d'une sous-suite vers le relèvement canonique. En pratique, on tire avantage de mises en formulations différentes de ces propriétés pour accélérer le calcul du relèvement canonique (voir [Ver03] pour une présentation détaillée et des comparaisons entre les différentes méthodes).

Une fois le relèvement canonique obtenu avec la précision souhaitée, on calcule les invariants absolus de la courbe C. Contrairement à la méthode complexe, on ne fait cela que pour une seule courbe. Afin de retrouver les polynômes de classes d'Igusa (ou tout au moins un des facteurs irréductibles sur $\mathbb{Q}$), on utilise l'algorithme LLL [4, Sec.4.2]. Pour éviter l'explosion combinatoire dans le choix des racines des polynômes H_m de l'étape (5), nous introduisons dans l'article deux nouveaux polynômes $\hat{H}_2$ et $\hat{H}_3$. Pour ces polynômes, (j_1, j_2, j_3) est un triplet d'invariants absolus si et seulement si

$$H_1(j_1) = 0, \quad H_1'(j_1)j_2 = \hat{H}_2(j_1), \quad H_1'(j_1)j_3 = \hat{H}_3(j_1).$$

Ces polynômes sont obtenus par une interpolation de Lagrange modifiée, laquelle a la propriété de conserver des coefficients pour $\hat{H}_m$ de même taille que ceux de H_m. Pour finir, on peut alors reprendre les étapes (4),(5) et (6) de la méthode complexe.

La complexité de l'algorithme est difficile à évaluer mais il est clair que le facteur limitant est la reconstruction des polynômes par LLL qui dépend du degré des polynômes et aussi de la taille de leurs coefficients. Au moment de la publication de l'article, on ne connaissait pas de borne pour celle-ci. Cependant, notre méthode permettait d'atteindre un nombre de classes de 50, à partir d'une courbe définie sur $\mathbb{F}_{32}$, alors que les records de la méthode complexe étaient de 10. Ceci est dû à l'un des avantages évidents de notre méthode qui est l'utilisation d'une arithmétique exacte. En revanche, un inconvénient de la méthode est que nos hypothèses sur la courbe $\tilde{C}$ nous contraignent à nous restreindre à certains K (ceux pour lesquels 2 est totalement décomposé). De plus, il faut reconnaître

les courbes $\tilde{C}$ pour lesquelles $\mathrm{End}(\mathrm{Jac}\,\tilde{C}) = \mathcal{O}_K$, ce qui devient délicat lorsque q est grand. Cette question est abordée dans la partie suivante.

5.4.3 Développements récents et questions ouvertes

De nombreux articles sont apparus sur ce thème depuis la publication de nos résultats. Dans [Koh08] et [CKL08], on trouve des généralisations en caractéristique $p \neq 2$ de la méthode p-adique et une méthode ℓ-adique avec $\ell \neq p$. Grâce à cette batterie d'algorithmes, Kohel construit une base de données des polynômes de classes d'Igusa pour les corps quartiques CM :

`http://echidna.maths.usyd.edu.au/kohel/dbs/complex_multiplication2.html`).

Une troisième alternative à la méthode complexe est née avec les articles [EL09], [FL08]. Les auteurs y proposent un algorithme basé sur le théorème des restes chinois. En genre 2, les complexités des différentes méthodes n'ont pas été établies mais dans le cas du genre 1, [BBEL08] montre que toutes les méthodes existantes ont des complexités similaires. Une autre contribution de ces articles est de proposer un algorithme probabiliste pour le calcul de l'anneau des endomorphismes des courbes de genre 2 ordinaires sur $\mathbb{F}_p$ avec $p > 3$. Sous ces hypothèses, ils montrent [FL08, Prop.3.7] que p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ où $\pi, \bar{\pi}$ sont respectivement l'endomorphisme de Frobenius et le Verschiebung de $\mathrm{Jac}\,\tilde{C}$. On calcule une $\mathbb{Z}[\pi, \bar{\pi}]$-base de $\mathcal{O}_K$ sous la forme de polynômes P_i en $\pi, \bar{\pi}$, divisés par des entiers d_i premiers à p. L'idée de base des algorithmes pour tester si l'anneau $\mathrm{End}(Jac(\tilde{C})) \simeq \mathcal{O}_K$ est de vérifier si $P_i(\pi, \bar{\pi})$ est nul sur la d_i-torsion. Si c'est le cas pour tout i, alors l'anneau des endomorphismes est maximal. Comme on l'a vu, dans notre algorithme, on souhaite également que $\mathrm{End}(\mathrm{Jac}\,\tilde{C}) \simeq \mathcal{O}_K$. Nous sommes dans un cadre d'application légèrement différent de celui permis par les algorithmes de *loc. cit.*, puisqu'il peut arriver que 2 divise $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$. Cependant, puisque la courbe est ordinaire, on peut adapter la méthode. À titre d'exemple, supposons $d = p^m \leq q$ et $f = P(\pi, \bar{\pi})/d \in \mathcal{O}_K$ avec $P \in \mathbb{Z}[x, y]$. En écrivant

$$P(x, y) = P_1(x) + yP_2(y) + xyP_3(x, y),$$

on a $f \in \mathrm{End}(\mathrm{Jac}\,\tilde{C})$ si et seulement si $P_1(\pi)$ et $\pi P_2(\pi) + P_1(0)$ sont nulles sur $(\mathrm{Jac}\,\tilde{C})[d](\bar{k})$. Ces méthodes restent toutefois coûteuses lorsque l'indice est divisible par un grand nombre premier. Développer une méthode déterministe dans l'esprit de [Koh96] serait souhaitable. G. Bisson, doctorant de P. Gaudry et T. Lange, et D. Grünenwald, postdoctorant à l'IML, travaillent sur ces questions.

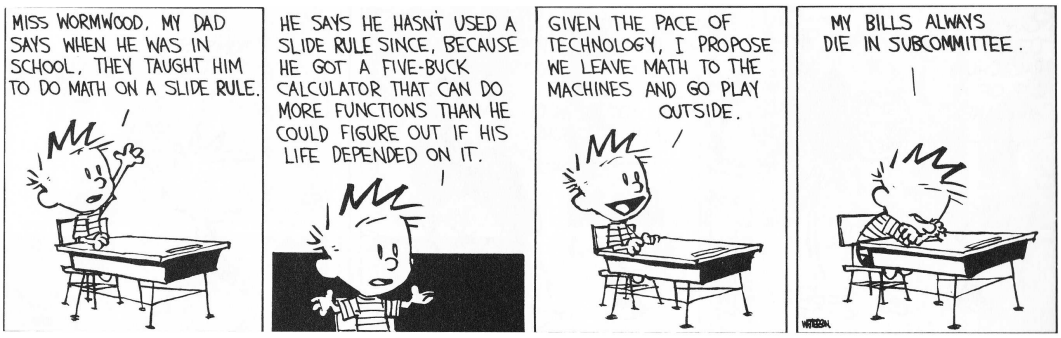
La méthode complexe a également connu un regain d'intérêt notamment grâce au travail de Dupont [Dup06] et de Houtmann (thèse en préparation). L'un des points clé est l'accélération du calcul des ThetaNullwerte à partir de la matrice des périodes. Pour cela, Dupont a interprété le calcul de la matrice des périodes à partir des ThetaNullwerte par l'AGM (voir section 4.5.3) comme une fonction et obtient ainsi les ThetaNullwerte comme les solutions d'une équation par une méthode de Newton. Néanmoins, la définition de "bonnes racines" pour assurer la convergence de la suite AGM reste délicate et

repose sur des résultats heuristiques. Il serait bon de revisiter le travail de Dupont et de le généraliser en dimension supérieure. On pourra commencer par comparer son travail à celui de [Jar08].

Récemment Streng [Str09] a proposé la première analyse de complexité d'une méthode CM complexe en genre 2. Pour cela, il a utilisé les travaux de Goren et Lauter [GL07] sur les bornes des dénominateurs des coefficients des polynômes H_i lorsque les premiers 2 et 3 ne sont pas ramifiés dans K. Il mentionne également l'existence de bornes plus fines dans [Yan07], malheureusement uniquement connues dans un nombre restreint de cas. Nos recherches sur les diviseurs des formes χ_h (voir section 4.5.1) auront peut-être des conséquences sur cette question.

Une autre question ouverte est la recherche d'analogues en genre 2 des invariants de classes tels que les fonctions de Weber ou de Weber généralisées. On pourra consulter `http://www.lix.polytechnique.fr/~morain/Exposes/fields09.pdf` pour un survol en genre 1. Cela permettrait, comme dans le cas elliptique, de diminuer la taille des coefficients des polynômes modulaires. Kohel a proposé récemment des "invariants de Richelot" qui permettent d'obtenir des résultats dans cette direction (voir l'exposé `http://echidna.maths.usyd.edu.au/kohel/doc/lower-cm.pdf`). Uzunkol [Uzu10] termine sa thèse sur ces questions.

La généralisation au genre 3 est également un sujet intéressant. Weng [Wen01] a réalisé ce projet dans les cas particuliers des courbes hyperelliptiques avec $K = K^+(i)$ où $i^2 = -1$ et avec Koike dans [KW05] pour $K = K^+(\zeta_3)$ avec $\zeta_3^2 + \zeta_3 + 1 = 0$. Ces courbes décrivent des familles de dimension 2 et on sait dans ces cas reconstruire une équation de la courbe en fonction des ThetaNullwerte. De plus, comme les équations des modèles dans ces familles ne dépendent chacune que de deux paramètres, la reconstruction à partir des invariants absolus peut être effectuée en résolvant le système algébrique par les bases de Gröbner. Si l'on souhaite généraliser cette méthode à tout le genre 3, les obstacles que nous rencontrons s'intègrent dans la problématique : invariants $\leftrightarrow$ courbe $\leftrightarrow$ jacobienne. La première "équivalence" est discutée dans la section 2.5.2 et la seconde dans la section 4.5.3.
Parmi les autres pistes à suivre, dans le cas non hyperelliptique, on pourrait réfléchir à remplacer les polynômes de classes des invariants absolus (à partir desquels la reconstruction demeure incertaine) par des polynômes de classes sur les 6 coordonnées libres d'un système d'Aronhold. Ces derniers étant reliés à $\mathsf{M}_{3,2}$, ceux-ci vivent généralement dans une extension $\mathrm{Sp}_6(\mathbb{F}_2)$ du corps des modules de la jacobienne. La question est donc de voir si sous certaines bonnes hypothèses sur K il serait possible d'imposer que la 2-torsion soit rationnelle. Remarquons enfin que l'extension de la méthode 2-adique ne pose pas de problème supplémentaire : la convergence par la méthode AGM fonctionne encore. On retrouve les deux variantes : soit la duplication sur les ThetaNullwerte comme dans [16], soit par un analogue de Richelot grâce aux formules de [9].



6 Appendice

In this appendix, we give the proofs of theorems 5.1.2 and 5.1.3.

6.1 Structure of the canonical divisor

In the following, we denote by $(x : y : z)$ the chosen coordinates in $\mathbb{P}^2$, and by (x, y) the coordinates in $\mathbb{A}^2$. Let $k = \mathbb{F}_q$ be a finite field with $q = p^n$ elements. When we want to state propositions valid over any field, we will use the letter K instead of k. We will further denote by $\bar{K}$ the algebraic closure of K.

Let C be a genus 3 non-hyperelliptic curve defined over a field K canonically embedded as a smooth plane quartic defined over K. For such a model, the positive canonical divisors of C are the intersection divisors of C with lines in $\mathbb{P}^2(\bar{K})$. Over $\bar{K}$, there are 5 possibilities for the intersection divisor $(l \cdot C) = P_1 + P_2 + P_3 + P_4$ of a line l with C:

1. The four points are pairwise distinct. This is the generic position.
2. $P_1 = P_2$, then l is tangent to C at P_1.
3. $P_1 = P_2 = P_3$. The point P_1 is then called a *flex*. As a linear intersection also represents the canonical divisor κ_C, these points are exactly the ones where a regular differential has a zero of order 3. The curve C has infinitely many flexes if and only if $\operatorname{char} K = 3$ and C is isomorphic to the Fermat quartic $x^4 + y^4 + z^4 = 0$ (which is also isomorphic to the Klein quartic $x^3y + y^3z + z^3x = 0$). If C has finitely many flexes, then these points are Weierstrass points and the sum of their weights is 24. Moreover the weight of a flex which is not a hyperflex (see point (5)) is 1 whereas a hyperflex has weight greater or equal to 2. If $\operatorname{char} K > 2$, then the weight of a hyperflex is exactly 2 ([Tor00, p.28]). See also [VlT05] for $\operatorname{char} K = 2$.

4. $P_1 = P_2$ and $P_3 = P_4$. The line l is called a *bitangent* of the curve C and the points P_i *bitangency points*. It is well known (see for instance [6', Sec.3.3.1]) that if $\operatorname{char} K \neq 2$ then C has exactly 28 bitangents. If $\operatorname{char} K = 2$, then C has respectively $7, 4, 2$, or 1 bitangents, according to the 2-rank of its Jacobian is respectively $3, 2, 1$ or 0 (see for example Part 2.1).
5. $P_1 = P_2 = P_3 = P_4$. The point P_1 is called a *hyperflex*. Generically, such a point does not exist. More precisely, the locus of quartics with at least one hyperflex is of codimension one in the moduli space M_3. The number of hyperflexes is less than 12 if C is not isomorphic to the Fermat quartic over a field of characteristic

3. Moreover in this later case, the number of hyperflexes of C is equal to 28 (all the bitangency points are hyperflexes) (see [Tor00, p.30]).

Some hyperflexes P can even be more special. Let $P \in C$ be a point and let us denote $\phi_P : C \to |\kappa_C - P| = \mathbb{P}^1$ the degree three map induced by the linear system $|\kappa_C - P|$. If this cover is Galois, such a point P is called a *Galois point*. They are studied in [MY00] in characteristic 0. In the following, we will denote by $\mathrm{Gal}\,(C)$ the set of Galois points of C.

Lemma 6.1.1. *Let C be a smooth plane quartic defined over an algebraically closed field K. The number of Galois points is at most 4 if $\mathrm{char}\, K \neq 3$ and at most 28 if $\mathrm{char}\, K = 3$.*

Proof. Let P be a Galois point of C. First we show that P is a hyperflex. If the cover ϕ_P is Galois then there exists an automorphism $\alpha : C \to C$ of order 3 which induces $\phi_P : C \to C/\langle\alpha\rangle$. As C is canonically embedded, α induces a projective automorphism of $\mathbb{P}^2$. We show that $\alpha(P) = P$. Let $R_1 + R_2 + R_3 = \phi_P^{-1}(t_0)$ for a generic point t_0. The line $\overline{\alpha(R_1)\alpha(R_2)}$ goes through $\alpha(P)$. The morphism α permutes the R_i's so

$$\overline{\alpha(R_1)\alpha(R_2)} = \overline{R_1R_2} \text{ and } \alpha(P) = P.$$

The point P is thus totally ramified in the cover ϕ_P. Therefore, the tangent line $T_P(C)$ cuts C at P with multiplicity 4, i.e. P is a hyperflex.
Now, if a point $Q \neq P$ is ramified then Q is completely ramified and it is then a flex. If $\mathrm{char}\, K \neq 3$, Hurwitz's formula shows that there must be exactly 4 such points associated to P. Let ω be the minimum of the weights of $P \in \mathrm{Gal}\,(C)$. According to Section 6.1 (3), $\omega \geq 2$. So we get $\#\mathrm{Gal}\,(C) \cdot (4 \cdot 1 + \omega) \leq 24$. Thus $\#\mathrm{Gal}\,(C) \leq 4$. This bound is reached for instance for $C : yz^3 + x^4 + z^4 = 0$ which has Galois points $(0:0:1), (0:c:1)$ with $c^3 = -1$.
If $\mathrm{char}\, K = 3$, Section 6.1 (5) shows that $\#\mathrm{Gal}\,(C) \leq 28$. We show that this bound is reached for the Fermat quartic $C : x^4 + y^4 + z^4 = 0$. Using Section 6.1 (3), we know that any point $P = (x_0 : y_0 : z_0) \in C$ is a flex. Moreover, the fourth intersection point of C with the tangent $T_P(C)$ is $(x_0^9 : y_0^9 : z_0^9)$, so P is a hyperflex if and only if $(x_0^9 : y_0^9 : z_0^9) = (x_0 : y_0 : z_0)$. Now suppose $z_0 = 1$ and let $X = x - x_0$, $Y = y - y_0$. We get

$$(X + x_0)^4 + (Y + y_0)^4 + 1 = X^4 + x_0^3X + x_0X^3 + Y^4 + y_0^3Y + y_0Y^3 = 0.$$

Let $Y = tX$. The cover ϕ_P defines an extension $K(C) = K(X,t)/K(t)$ with equation

$$f = X^3(1 + t^4) + X^2(x_0 + y_0t^3) + (x_0^3 + ty_0^3).$$

This cover is Galois if and only if

$$\mathrm{Disc}_X(f) = \begin{cases} -x_0^6 & \text{if } y_0 = 0\,, \\ -y_0^6 \cdot \left(t + \left(\frac{x_0}{y_0}\right)^{-1/3}\right)^9 \cdot \left(t + \left(\frac{x_0}{y_0}\right)^3\right) & \text{otherwise}\,, \end{cases}$$

is a square in $K(t)$. It is easy to see that this is the case if $y_0 = 0$ or $(x_0/y_0)^9 = x_0/y_0$. Obviously, if P is a hyperflex of C, it satisfies this condition. So the bound is reached. □

Remark 6.1.2. It is not clear what the maximum of $\#\mathrm{Gal}\,(C)$ can be when, in characteristic 3, C is not isomorphic to the Fermat quartic. According to Section 6.1 (5) there are at most 12 hyperflexes but I do not know if this number can be reached. Moreover, wild ramification prevents us from using Hurwitz's formula as easily as in Lemma 6.1.1. In particular, if the curve has 3-rank 0, then a Galois cover ϕ_P is (wildly) ramified at P only. The only other tricky case (using Deuring-Safarevic formula [Sub75, th.4.2]) may be the case where the 3-rank is equal to 2. In such a case we have two points wildly ramified.

In the sequel, we will need the following lemma.

Lemma 6.1.3. *Let C be a smooth plane quartic defined over an algebraically closed field K. There is always a bitangency point which is not a hyperflex unless*

1. $\mathrm{char}\, K = 2$ *and* $\mathrm{Jac}\, C$ *is supersingular,*
2. $\mathrm{char}\, K = 2$ *and C is isomorphic to a 2-rank one quartic*
$$(ax^2 + by^2 + cz^2 + dxy)^2 + xy(y^2 + xz) = 0$$
with $ac \neq 0$,
3. $\mathrm{char}\, K = 2$ *and C is isomorphic to a 2-rank two quartic*
$$(ax^2 + by^2 + cz^2)^2 + xyz(y + z) = 0$$
with $abc \neq 0$ and $b + c \neq 0$,
4. $\mathrm{char}\, K = 3$ *and C is isomorphic to the Fermat quartic.*

Proof. According to Section 6.1 (5), the number of hyperflexes when C is not isomorphic to the Fermat quartic and $\mathrm{char}\, K = 3$, is less than 12. On the other hand, if $p \neq 2$, a curve C has 28 bitangents, and thus there are at least 8 bitangency points which are not hyperflexes. However, for the Fermat quartic in characteristic 3, all bitangency points are hyperflexes.
There remains to look at the case $p = 2$ for which we use the classification of [Wal95], [11] (see Part 2.1). The quartic C falls into four categories according to its number of bitangents:

1. if C has only one bitangent, then C is isomorphic to a model $Q^2 = x(y^3 + x^2z)$ where $Q = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$ and $c \neq 0$. The unique bitangent $x = 0$ cuts C at points $(x : y : z)$ satisfying $by^2 + cz^2 + eyz = 0$. Therefore, C has a hyperflex if and only if $e = 0$, i.e. C falls into the subfamily $\mathcal{S}$ [11, p.468] of curves whose Jacobian is supersingular.
2. if C has two bitangents, then C is isomorphic to a model $Q^2 = xy(y^2 + xz)$ where $Q = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$ and $ac \neq 0$. All bitangency points are then hyperflexes if and only if $e = f = 0$.
3. if C has four bitangents, then C is isomorphic to $Q^2 = xyz(y + z)$ with
$$Q = ax^2 + by^2 + cz^2 + dxy + eyz + fzx \text{ and } abc \neq 0, b + c + e \neq 0.$$
All bitangency points are hyperflexes if and only if $d = e = f = 0$.

4. if C has seven bitangents, then C is isomorphic to $Q^2 = xyz(x+y+z)$ with $Q = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$ and some additional conditions on the coefficients [11, p.445]. The bitangents are

$$\{x, y, z, x+y+z, x+y, y+z, x+z\}.$$

Suppose that the intersection points of $x = 0$, $y = 0$ and $z = 0$ with C are hyperflexes, then $d = e = f = 0$. Moreover $x + y = 0$ gives a hyperflex if and only if $(a+b)y^2 + yz + cz^2$ is a perfect square, which is never possible.

□

6.2 Proof of theorem 5.1.2

Let C be a smooth plane quartic defined over a finite field k. We denote by $(*)$ the condition: there is a line which cuts the quartic C at 4 rational points (distinct or not).

We want to prove that, if $q \geq 127$, then the condition $(*)$ is fulfilled. Note that, as an easy consequence of Hasse-Weil bound, we can assume that C has a rational point P. We follow the same lines as [DT08, p.604]. Let κ_C be the canonical divisor of C. The lines intersecting C at P are in bijection with the divisors in the complete linear system $|\kappa_C - P|$. We wish to estimate the number of completely split divisors in this linear system using an effective Chebotarev density theorem for function fields, as in [KMS94, Th.1]. In order to do so, we consider the separable geometric cover $\phi = \phi_P : C \to |\kappa_C - P| = \mathbb{P}^1$ of degree 3 induced by the linear system $|\kappa_C - P|$. We may assume that no rational point in $\mathbb{P}^1$ is ramified. Otherwise, it is easy to see that the fibre of ϕ above this point has only rational points and the condition $(*)$ is fulfilled. Theorem [KMS94, Th.1] assumes that the cover is Galois but we can use the following easy lemma.

Lemma 6.2.1. *Let K/F be a finite separable extension of function fields over a finite field k. Let L be the Galois closure of K/F. A place of F splits completely in K if and only if it splits completely in L.*

Proof. It is clear that, if a place $P \in F$ splits completely in L, it splits completely in K. Conversely, let G be the Galois group of L/F and H be the Galois subgroup of L/K. By construction (see [Bou06, A.V.p.54]), L is the compositum of the conjugates K^σ with $\sigma \in G/H$. If a place $P \in F$ splits completely in K, it splits completely in each of the K^σ. It is then enough to apply [Sti93, Cor.III.8.4] to conclude. □

We then get a similar result to [DT08].

Proposition 6.2.2. *Let C be a smooth plane quartic defined over k.*

1. *If the cover ϕ has a non-trivial automorphism, then the number N of completely split divisors in $|\kappa_C - P|$ satisfies*

$$\left| N - \frac{q+1}{3} \right| \leq 2\sqrt{q} + |D|$$

where $|D| = \sum_{y \in \mathbb{P}^1, ramified} \deg y$.

2. *If the cover ϕ has a non-trivial $\bar{k}$-automorphism not defined over k, then there are no completely split divisors in $|\kappa_C - P|$.*
3. *If the cover ϕ has no non-trivial automorphism, then the number N of completely split divisors in $|\kappa_C - P|$ satisfies*

$$\left| N - \frac{q+1}{6} \right| \leq \sqrt{q} + |D|.$$

To avoid case (2), we need to bound the number of points $P \in C(\bar{k})$ such that the cover $\phi_P : C \to \mathbb{P}^1$ is geometrically Galois. This is given by lemma 6.1.1. Moreover, it is easy to bound $|D|$ using Hurwitz's formula :

$$|D| \leq (2 \cdot 3 - 2) - 3 \cdot (0 - 2) = 10.$$

Thus to get a line satisfying $(*)$, it is enough to have

$$\begin{cases} \#C(k) & > \#\operatorname{Gal}(C), \\ \frac{q+1}{6} & > \sqrt{q} + 10. \end{cases}$$

This concludes the proof.

6.3 Proof of theorem 5.1.3

Let C be a smooth plane quartic defined over a field K. We denote by $(*)$ the condition: there exists a tangent to the quartic C which cuts C at rational points only.

Let $T : C \to \mathrm{Sym}^2(C)$ be the "*tangential correspondence*" which sends P to the divisor $(T_P(C) \cdot C) - 2P$. We associate to T its correspondence curve

$$X_C = \{(P, Q) \in C \times C : Q \in T(P)\}$$

which is defined over K. We denote by π_i, $i = 1, 2$, the projections on the first and second factor. The morphism $\pi_1 : X_C \to C$ is a 2-cover between these two projective curves.

Lemma 6.3.1. *Let K be an algebraically closed field. The projection $\pi_1 : X_C \longrightarrow C$ has the following properties :*

1. *The ramification points of π_1 are the bitangency points of C,*
2. *ϕ is separable,*
3. *The point $(P, Q) \in X_C$ such that P, Q are bitangency points and P is not a hyperflex (i.e. $P \neq Q$) is a regular point if and only if* $\operatorname{char} K \neq 2$,
4. *If* $\operatorname{char} K \neq 2$, *the only possible singular points of X_C are the points (P, P) where P is a hyperflex of C.*

Proof. The first property is an immediate consequence of the definition of a bitangent. If π_1 is not separable then $\operatorname{char} K = 2$ and ϕ is purely inseparable. Thus $\#\phi^{-1}(P) = 1$ for all $P \in C$, i.e. all P are bitangency points. This is impossible since the number of bitangents is finite (less or equal to 7).
Let $F(x, y, z) = 0$ be an equation of C. Let $Q \neq P$ be a point of C defining a point (P, Q) in $X_C \setminus \Delta$ where Δ is the diagonal of $C \times C$. For such points, it is easy to write local equations as follows. We can suppose that $P = (0 : 0 : 1) = (0, 0)$, $Q = (1 : 0 : 1) = (1, 0)$ and assume that $f(x, y) = F(x, y, 1)$ is an equation of the affine part of C. Then, if we consider the curve Y_C in $\mathbb{A}^4(x, y, z, t)$ defined by

$$\begin{cases} f(x,y) & = 0\,, \\ f(z,t) & = 0\,, \\ \frac{\partial f}{\partial x}(x,y)(z-x) + \frac{\partial f}{\partial y}(x,y)(t-y) & = 0\,, \end{cases}$$

it is clear that $Y_C \setminus \Delta$ is an open subvariety of X_C containing (P, Q). The Jacobian matrix at the point $(P, Q) = ((0, 0), (1, 0))$ is equal to

$$\begin{pmatrix} \frac{\partial f}{\partial x}(0,0) & 0 & \frac{\partial^2 f}{\partial x^2}(0,0) - \frac{\partial f}{\partial x}(0,0) \\ \frac{\partial f}{\partial y}(0,0) & 0 & \frac{\partial^2 f}{\partial x \partial y}(0,0) - \frac{\partial f}{\partial y}(0,0) \\ 0 & \frac{\partial f}{\partial x}(1,0) & \frac{\partial f}{\partial x}(0,0) \\ 0 & \frac{\partial f}{\partial y}(1,0) & \frac{\partial f}{\partial y}(0,0) \end{pmatrix}.$$

Now, if P and Q are bitangency points, then the tangent at these points is $y = 0$, so $\frac{\partial f}{\partial x}(0, 0) = \frac{\partial f}{\partial x}(1, 0) = 0$. The only non-trivially zero minor determinant of the matrix is then

$$\frac{\partial f}{\partial y}(1,0) \cdot \frac{\partial f}{\partial y}(0,0) \cdot \frac{\partial^2 f}{\partial x^2}(0,0).$$

So $(P, Q) \in X_C$ is not singular if and only if $\frac{\partial^2 f}{\partial x^2}(0, 0) \neq 0$. This can never be the case if $\operatorname{char} K = 2$, so we suppose that $\operatorname{char} K \neq 2$. We can always assume that the point $(0 : 1 : 0) \notin C$ and we write

$$f(x, y) = x^4 + x^3 h_1(y) + x^2 h_2(y) + x h_3(y) + h_4(y)\,,$$

where h_i are polynomials (in one variable) over K of degree $\leq i$. Since $y = 0$ is a bitangent at P and Q, we have

$$f(x, 0) = x^2(x - 1)^2 = x^4 - 2x^3 + x^2\,,$$

and thus $h_2(0) = 1$. Now

$$\frac{\partial^2 f}{\partial x^2}(0, 0) = 2h_2(0) \neq 0.$$

Finally if $(P, Q) \in X_C$ is not ramified, it is a smooth point. This proves the last assertion. □

Remark 6.3.2. In characteristic 0, it is known that the points (P, P) such that P is a hyperflex of C are ordinary double points. We conjecture that this is also true if and only if $\operatorname{char} K \neq 2$.

To see whether X_C is geometrically irreducible, we use the following easy lemma for which we could not find a reference.

Lemma 6.3.3. *Let $\phi : X \to Y$ be a separable morphism of degree 2 between two projective curves defined over an algebraically closed field K such that*

1. *Y is smooth and irreducible,*
2. *there exists a point $P_0 \in Y$ such that ϕ is ramified at P_0 and $\phi^{-1}(P_0)$ is not singular.*

Then X is irreducible.

Proof. Let $s : \tilde{X} \to X$ be the normalization of X and $\tilde{\phi} = \phi \circ s : \tilde{X} \to Y$. Due to the second hypothesis, $\tilde{\phi} : \tilde{X} \to Y$ is a separable, ramified 2-cover. Clearly, X is absolutely irreducible if and only if $\tilde{X}$ is.
Let us assume that $\tilde{X}$ is not irreducible. There exist smooth projective curves $\tilde{X}_1$ and $\tilde{X}_2$ such that $\tilde{X} = \tilde{X}_1 \cup \tilde{X}_2$. Then, consider for $i = 1, 2$, $\tilde{\phi}_i = \tilde{\phi}_{|\tilde{X}_i} : \tilde{X}_i \to Y$. Each of these morphisms is of degree 1 and since the curves are projective and smooth, they define an isomorphism between $\tilde{X}_i$ and Y.
Since $P_0 \in Y$ is a ramified point, $\tilde{\phi}_1^{-1}(P_0) = \tilde{\phi}_2^{-1}(P_0)$. It follows that $\tilde{\phi}^{-1}(P_0) \in \tilde{X}_1 \cap \tilde{X}_2$ so that $\tilde{\phi}^{-1}(P_0)$ is singular, which contradicts the hypothesis. □

Now, let us assume that $K = k$ is a finite field. We want to prove that, for $q \geq 66^2 + 1$ and $p \neq 2$, there is a rational point on X_C, i.e. there is $(P, Q) \in C(\mathbb{F}_q)^2$ such that $(T_P(C) \cdot C) = 2P + Q + R$ for some point $R \in C(\mathbb{F}_q)$. Thus, the tangent $T_P(C)$ satisfies then the condition $(*)$. We will need the following proposition.

Proposition 6.3.4 ([AP95])**.** *Let X be a geometrically irreducible curve of arithmetic genus π_X defined over $\mathbb{F}_q$. Then*

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2\pi_X\sqrt{q}.$$

In particular if $q \geq (2\pi_X)^2$ then X has a $\mathbb{F}_q$-rational point.

We can now prove the theorem. We assumed that the characteristic of k is different from 2.
Let us first start with the Klein quartic in characteristic 3. We know that all its points are flexes. So if there exists $P \in C(k)$, then the tangent at P cuts C at P and at another unique point which is again rational over k. So the condition $(*)$ is satisfied. Now when $q > 23$ and $q \neq 29, 32$, it is proved in [HLT05] that a genus 3 non-hyperelliptic curve over $\mathbb{F}_q$ has always a rational point and the result follows.
We suppose that C is a smooth plane quartic not $\bar{k}$-isomorphic to the Klein quartic if $p = 3$. As we assumed that $\operatorname{char} \mathbb{F}_q \neq 2$, by Lemma 6.3.3 and Lemma 6.3.1, we conclude that X_C is an absolutely irreducible projective curve. Moreover, if we assume that C has no hyperflex, then X_C is smooth and we can compute its genus using Hurwitz's formula for the 2-cover $\pi_1 : X_C \to C$ ramified over the $2 \cdot 28$ bitangency points. In fact,

$$2g_{X_C} - 2 = 2(2 \cdot 3 - 2) + 56$$

and thus $g_{X_C} = 33$. As the arithmetic genus π_{X_C} is constant in flat families, we get that $\pi_{X_C} = 33$ for any curve C. We can now use Proposition 6.3.4 to get the bound.

Remark 6.3.5. Another possibility is to use the theory of correspondences : T is a correspondence with valence $\nu = 2$, i.e. the linear equivalence class of $T(P) + \nu P$ is independent of P. If we denote by E (resp. F) a fiber of π_1 (resp. π_2), we get as in the proof of [GH94, p.285] that $X \sim aE + bF - \nu\Delta$ for some $a, b \in \mathbb{Z}$ to be determined. Note that (see for instance [Har77, ex.III.8.3], [Har77, ex.V.1.6])

$$\begin{cases} E.E = F.F & = 0, \\ E.F = \Delta.E = \Delta.F & = 1, \\ \kappa_{C\times C} & \equiv_{\text{num}} (2g-2)E + (2g-2)F, \\ \Delta^2 & = (2-2g). \end{cases}$$

Moreover $\deg \pi_1 = X_C.E = b - \nu = 2$ and $\deg \pi_2 = X_C.F = a - \nu$. The degree of π_2 is equal to the degree of the dual curve C^* minus 2. For any non singular plane curve C of degree d, one has ([Hom93, p.786])

$$\deg C^* = \frac{d(d-1)}{m}$$

where m is the inseparable degree of the dual map $C \to C^*$. The degree m equals 1 except if $\operatorname{char} k = 3$ where C is geometrically isomorphic to the Klein quartic (then $m = 3$) or if $\operatorname{char} k = 2$ (then $m = 2$) (see [Hom89, Cor.2.4]).
We can compute the arithmetic genus of X_C thanks to the adjunction formula [Har77, ex.V.1.3]

$$2\pi_{X_C} - 2 = X_C.(X_C + \kappa_{C\times C}).$$

We find

$$\pi_{X_C} = ab + (g-1)(a + b - 2\nu - \nu^2) - \nu(a+b) + 1.$$

Computing the different intersection numbers, one finds again $\pi_{X_C} = 33$ if $p \neq 2$ and if C is not $\bar{k}$-isomorphic to the Klein quartic in characteristic 3. However, we still do not know whether X_C is absolutely irreducible in characteristic 2.

Bibliographie générale

[AAMZ09] E. Alekseenko, S. Aleshnikov, N. Markin & A. Zaytsev – « Optimal curves of genus 3 over finite fields with discriminant -19 », 2009.

[Abh63] S. Abhyankar – « Remark on Hessians and flexes », *Nieuw Arch. Wisk. (3)* **11** (1963), p. 110–117.

[ACGH85] E. Arbarello, M. Cornalba, P. Griffiths & J. Harris – *Geometry of algebraic curves, vol. I*, vol. 267, Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, New-York, 1985.

[AP95] Y. Aubry & M. Perret – « A Weil theorem for singular curves », in *Proceedings of arithmetic, geometry and coding theory*, vol. IV, ed. Pellikaan, Perret, Vlăduţ De Gruyter, 1995, p. 1–7.

[Arè08] C. Arène – « Étude d'un nouveau modèle pour les courbes elliptiques », Mémoire de Master à l'Institut de Mathématiques de Luminy, Marseille, 2008.

[Aro50] S. Aronhold – « Zur Theorie der homogenen Functionen dritten Grades von drei Variablen. », *J. Reine Angew. Math.* **39** (1850), p. 140–159.

[AT02] R. Auer & J. Top – « Some genus 3 curves with many points », in *Algorithmic number theory (Sydney, 2002)*, Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, p. 163–171.

[Bar06] F. Bars – « Automorphism groups of genus 3 curves », Notes del seminari Corbes de Gèneres 3, 2006.

[BBEL08] J. Belding, R. Bröker, A. Enge & K. Lauter – « Computing Hilbert class polynomials », in *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, p. 282–295.

[BBJ+08] D. J. Bernstein, P. Birkner, M. Joye, T. Lange & C. Peters – « Twisted Edwards curves », in *Africacrypt*, 2008, `http://cr.yp.to/papers.html#twisted`, p. 389–405.

[Bed07] L. Bedratyuk – « On complete system of invariants for the binary form of degree 7 », *Journal of Symbolic Computation* **42** (2007), p. 935.

[Ben93] D. J. Benson – *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series, vol. 190, Cambridge University Press, Cambridge, 1993.

[Ben98] — , *Representations and cohomology. I*, second éd., Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1998, Basic representation theory of finite groups and associative algebras.

[Ber01] J. Bergström – « Master's thesis », Thèse, Kungl. Tekniska Högskolan, Stockholm, 2001.

[BG01] B. W. Brock & A. Granville – « More points than expected on curves over finite field extensions », *Finite Fields Appl.* **7** (2001), no. 1, p. 70–91, Dedicated to Professor Chao Ko on the occasion of his 90th birthday.

[BK86] E. Brieskorn & H. Knörrer – *Plane algebraic curves*, Birkhäuser Verlag, Basel, 1986, Translated from the German by John Stillwell.

[BL95] W. Bosma & H. Lenstra – « Complete systems of two addition laws for elliptic curves. », *J. Number Theory* **53** (1995), no. 2, p. 229–240.

[BL04] C. Birkenhake & H. Lange – *Complex abelian varieties*, second éd., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[BL07] D. J. Bernstein & T. Lange – « Faster addition and doubling on elliptic curves », in *ASIACRYPT 2007*, 2007, `http://cr.yp.to/newelliptic/`, p. 29–50.

[BLRF08] D. J. Bernstein, T. Lange & R. Rezaeian Farashahi – « Binary edwards curves », in *CHES '08 : Proceeding sof the 10th international workshop on Cryptographic Hardware and Embedded Systems* (Berlin, Heidelberg), Springer-Verlag, 2008, p. 244–265.

[Bou06] N. Bourbaki – *Elements of mathematics. commutative algebra. chapters 5–7. (éléments de mathématique. algèbre commutative. chapitres 5 à 7.) reprint of the 1985 original.*, Berlin : Springer., 2006.

[Bru08] N. Bruin – « The arithmetic of Prym varieties in genus 3 », *Compos. Math.* **144** (2008), no. 2, p. 317–338.

[BS04] R. Bröker & P. Stevenhagen – « Elliptic curves with a given number of points », in *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, p. 117–131.

[Car04] R. Carls – « A generalized arithmetic geometric mean », Thèse, Rijksuniversiteit Groningen, 2004.

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen & F. Vercauteren (éds.) – *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[CH02] J.-M. Couveignes & T. Henocq – « Action of modular correspondences around CM points », in *Algorithmic number theory (Sydney, 2002)*, Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, p. 234–243.

[Cha86] C.-L. Chai – « Siegel moduli schemes and their compactifications over **C** », in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986, p. 231–251.

[Cia99] E. Ciani – « I varii tipi possibili di quartiche piane più volte omologico-armoniche. », *Palermo Rend.* **13** (1899), p. 347–373.

[CKL08] R. Carls, D. Kohel & D. Lubicz – « Higher-dimensional 3-adic CM construction », *J. Algebra* **319** (2008), no. 3, p. 971–1006.

[CL06] A. Chambert-Loir – « Compter (rapidement) le nombre de solutions d'équations dans les corps finis », *séminaire BOURBAKI* **968** (2006), p. 1–48, `http://arxiv.org/abs/math/0611584v2`.

[CN07] G. Cardona & E. Nart – « Zeta function and cryptographic exponent of supersingular curves of genus 2 », in *Pairing-based cryptography—Pairing 2007*, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, p. 132–151.

[CNP05] G. Cardona, E. Nart & J. Pujolàs – « Curves of genus two over fields of even characteristic », *Math. Zeitschrift* **250** (2005), p. 177–201.

[Cox84] D. A. Cox – « The arithmetic-geometric mean of Gauss », *Enseign. Math. (2)* **30** (1984), no. 3-4, p. 275–330.

[CQ05] G. Cardona & J. Quer – « Field of moduli and field of definition for curves of genus 2 », in *Computational aspects of aglebraic curves* (Hackensack, NJ,), Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., 2005, p. 71–83.

[CS03] L. Caporaso & E. Sernesi – « Characterizing curves by their odd theta-characteristics », *J. Reine Angew. Math.* **562** (2003), p. 101–135.

[Del69] P. Deligne – « Variétés abéliennes ordinaires sur un corps fini », *Invent. Math.* **8** (1969), p. 238–243.

[Deu41] M. Deuring – « Die Typen der Multiplikatorenringe elliptischer Funktionenkörper », *Abh. Math. Sem. Hansischen Univ.* **14** (1941), p. 197–272.

[Die06] C. Diem – « An index calculus algorithm for plane curves of small degree », in *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, p. 543–557.

[Dix87] J. Dixmier – « On the projective invariants of quartic plane curves », *Adv. in Math.* **64** (1987), p. 279–304.

[dJ07] R. de Jong – « Explicit Mumford isomorphism for hyperelliptic curves », *J. Pure Appl. Algebra* **208** (2007), no. 1, p. 1–14.

[DK02] H. Derksen & G. Kemper – *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, Encyclopaedia of Mathematical Sciences, 130.

[DL03] I. Duursma & H.-S. Lee – « Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$ », in *Advances in cryptology—ASIACRYPT*

2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, p. 111–123.

[DM69] P. Deligne & D. Mumford – « The irreducibility of the space of curves of given genus », *Inst. Hautes Études Sci. Publ. Math.* (1969), no. 36, p. 75–109.

[DO88] I. Dolgachev & D. Ortland – « Point sets in projective spaces and theta functions », *Astérisque* (1988), no. 165, p. 210 pp. (1989).

[dSG97] E. de Shalit & E. Z. Goren – « On special values of theta functions of genus two », *Ann. Inst. Fourier (Grenoble)* **47** (1997), no. 3, p. 775–799.

[DT08] C. Diem & E. Thomé – « Index calculus in class groups of non-hyperelliptic curves of genus three », *J. Cryptology* **21** (2008), no. 4, p. 593–611.

[Dup06] R. Dupont – « Moyenne arithmético-géométrique, suites de Borchardt et applications », Thèse, Ecole polytechnique, Palaiseau, France, 2006.

[DvH01] B. Deconinck & M. van Hoeij – « Computing Riemann matrices of algebraic curves », *Phys. D* **152/153** (2001), p. 28–46, Advances in nonlinear mathematics and science.

[Edw07] H. M. Edwards – « A normal form for elliptic curves », *Bulletin of the American Mathematical Society* **44** (2007), p. 393–422, `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html`.

[EL09] K. Eisenträger & K. Lauter – « A CRT algorithm for constructing genus 2 curves over finite fields », in *Arithmetic, Geometry and Coding Theory, AGCT-10*, SMF, 2009, to appear.

[ER08] V. Enolskii & P. Richter – « Periods of hyperelliptic integrals expressed in terms of θ-constants by means of Thomae formulae », *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **366** (2008), no. 1867, p. 1005–1024.

[FC90] G. Faltings & C.-L. Chai – *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990, With an appendix by David Mumford.

[FL08] D. Freeman & K. Lauter – « Computing endomorphism rings of Jacobians of genus 2 curves over finite fields », in *Algebraic geometry and its applications*, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, p. 29–66.

[FST06] D. Freeman, M. Scott & E. Teske – « A taxonomy of pairing-friendly elliptic curves », Cryptology ePrint Archive, Report 2006/372, 2006, update 2008, `http://eprint.iacr.org/`.

[Gal01] S. D. Galbraith – « Supersingular curves in cryptography », in *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, p. 495–513.

[GGR05] J. González, J. Guàrdia & V. Rotger – « Abelian surfaces of GL_2-type as Jacobians of curves », *Acta Arith.* **116** (2005), no. 3, p. 263–287.

[GH94] P. Griffiths & J. Harris – *Principles of algebraic geometry*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1994, Reprint of the 1978 original.

[GH97] S. P. Glasby & R. B. Howlett – « Writing representations over minimal fields », *Comm. Algebra* **25** (1997), no. 6, p. 1703–1711.

[GH04] B. H. Gross & J. Harris – « On some geometric constructions related to theta characteristics », in *Contributions to automorphic forms, geometry, and number theory*, Johns Hopkins Univ. Press, Baltimore, MD, 2004, p. 279–311.

[Giz07] M. Gizatullin – « On covariants of plane quartic associated to its even theta characteristic », in *Algebraic geometry*, Contemp. Math., vol. 422, Amer. Math. Soc., Providence, RI, 2007, p. 37–74.

[GK06] M. Girard & D. R. Kohel – « Classification of genus 3 curves in special strata of the moduli space. », Hess, Florian (ed.) et al., Algorithmic number theory. 7th international symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 4076, 346-360 (2006)., 2006.

[GKZ94] I. M. Gel′fand, M. M. Kapranov & A. V. Zelevinsky – *Discriminants, resultants, and multidimensional determinants*, Mathematics : Theory & Applications, Birkhäuser Boston Inc., Boston, MA, 1994.

[GL06] E. Z. Goren & K. E. Lauter – « Evil primes and superspecial moduli », *Int. Math. Res. Not.* (2006), p. Art. ID 53864, 19.

[GL07] — , « Class invariants for quartic CM fields », *Ann. Inst. Fourier (Grenoble)* **57** (2007), no. 2, p. 457–480.

[Gor97] E. Z. Goren – « On certain reduction problems concerning abelian surfaces », *Manuscripta Math.* **94** (1997), no. 1, p. 33–43.

[GP08] S. D. Galbraith & K. G. Paterson (éds.) – *Pairing-based cryptography - pairing 2008, second international conference, egham, uk, september 1-3, 2008, proceedings*, Lecture Notes in Computer Science, vol. 5209, Berlin, Springer, 2008.

[GR04] S. D. Galbraith & V. Rotger – « Easy decision Diffie-Hellman groups », *LMS J. Comput. Math.* **7** (2004), p. 201–218 (electronic).

[Gra88] D. Grant – « A generalization of Jacobi's derivative formula to dimension two », *J. Reine Angew. Math.* **392** (1988), p. 125–136.

[Gro71] A. Grothendieck – *Revêtements étales et géométrie algébrique (SGA 1)*, Lecture Notes in Math., vol. 224, Springer-Verlag, Heidelberg, 1971.

[GSS05] J. Gutierrez, D. Sevilla & T. Shaska – « Hyperelliptic curves of genus 3 with prescribed automorphism group », in *Computational aspects*

of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, p. 109–123.

[Guà02] J. Guàrdia – « Jacobian nullwerte and algebraic equations », *J. Algebra* **253** (2002), no. 1, p. 112–132.

[Guà07] — , « Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves », *Ann. Inst. Fourier (Grenoble)* **57** (2007), no. 4, p. 1253–1283.

[Guà09] — , « On the torelli problem and jacobian nullwerte in genus three », 2009, `http://arxiv.org/abs/0901.4376`.

[Har77] R. Hartshorne – *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hen76] H.-W. Henn – « Die Automorphismengruppen der algebraischen Funktionenkorper vom Geschlecht 3 », 1976.

[HI83] K.-i. Hashimoto & T. Ibukiyama – « On class numbers of positive definite binary quaternion Hermitian forms. I,II,III », *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **27,28,30** (1980,1981,1983), p. 549–601, 695–699,393–401.

[HL03] E. W. Howe & K. E. Lauter – « Improved upper bounds for the number of points on curves over finite fields », *Ann. Inst. Fourier (Grenoble)* **53** (2003), no. 6, p. 1677–1737.

[HLP00] E. W. Howe, F. Leprévost & B. Poonen – « Large torsion subgroups of split Jacobians of curves of genus two or three. », *Forum Math.* **12** (2000), no. 3, p. 315–364.

[HLT05] E. W. Howe, K. E. Lauter & J. Top – « Pointless curves of genus three and four », in *Algebra, Geometry, and Coding Theory (AGCT 2003) (Y. Aubry and G. Lachaud, eds.)*, Séminaires et Congrès, vol. 11, Société Mathématique de France, Paris, 2005.

[HN65] T. Hayashida & M. Nishi – « Existence of curves of genus two on a product of two elliptic curves », *J. Math. Soc. Japan* **17** (1965), p. 1–16.

[Hof91] D. W. Hoffmann – « On positive definite Hermitian forms », *Manuscripta Math.* **71** (1991), no. 4, p. 399–429.

[Hom89] M. Homma – « A souped-up version of pardini's theorem and its application to funny curves. », *Compos. Math.* **71** (1989), p. 295–302.

[Hom93] — , « On duals of smooth plane curves. », *Proc. Am. Math. Soc.* **118** (1993), p. 785–790.

[Hon68] T. Honda – « Isogeny classes of abelian varieties over finite fields », *J. Math. Soc. Japan* **20** (1968), p. 83–95.

[How95] E. W. Howe – « Principally polarized ordinary abelian varieties over finite fields », *Trans. Amer. Math. Soc.* **347** (1995), no. 7, p. 2361–2401.

[How96] — , « Kernels of polarizations of abelian varieties over finite fields », *J. Algebraic Geom.* **5** (1996), no. 3, p. 583–608.

[How01] — , « Isogeny classes of abelian varieties with no principal polarizations », in *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math., vol. 195, Birkhäuser, Basel, 2001, p. 203–216.

[How04] — , « On the non-existence of certain curves of genus two », *Compos. Math.* **140** (2004), no. 3, p. 581–592.

[How08] — , « Supersingular genus-2 curves over fields of characteristic 3 », in *Computational arithmetic geometry*, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, p. 49–69.

[Hug05] B. Huggins – « Fields of moduli and fields of definition of curves », Thèse, University of California, Berkeley, Berkeley, California, 2005, http ://arxiv.org/abs/math.NT/0610247.

[Hug07] — , « Fields of moduli of hyperelliptic curves », *Math. Res. Lett.* **14** (2007), no. 2, p. 249–262.

[HZ02] E. W. Howe & H. J. Zhu – « On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field », *J. Number Theory* **92** (2002), no. 1, p. 139–163.

[Ibu89] T. Ibukiyama – « On automorphism groups of positive definite binary quaternion Hermitian lattices and new mass formula », in *Automorphic forms and geometry of arithmetic varieties*, Adv. Stud. Pure Math., vol. 15, Academic Press, Boston, MA, 1989, p. 301–349.

[Ibu93] — , « On rational points of curves of genus 3 over finite fields », *Tohoku Math. J. (2)* **45** (1993), no. 3, p. 311–329.

[Ich95] — , « Teichmüller modular forms of degree 3 », *Amer. J. Math.* **117** (1995), no. 4, p. 1057–1061.

[Ich96] — , « Theta constants and Teichmüller modular forms », *J. Number Theory* **61** (1996), no. 2, p. 409–419.

[Ich00] — , « Generalized Tate curve and integral Teichmüller modular forms », *Amer. J. Math.* **122** (2000), no. 6, p. 1139–1174.

[Igu60] J.-i. Igusa – « Arithmetic variety of moduli for genus two. », *Ann. Math* **72** (1960), p. 612–649.

[Igu62] — , « On Siegel modular forms of genus two », *Amer. J. Math.* **84** (1962), p. 175–200.

[Igu64] — , « On Siegel modular forms of genus two. II », *Amer. J. Math.* **86** (1964), p. 392–412.

[Igu67] — , « Modular forms and projective invariants », *Amer. J. Math.* **89** (1967), p. 817–855.

[Igu72] — , *Theta functions*, Springer-Verlag, New York, 1972, Die Grundlehren der mathematischen Wissenschaften, Band 194.

[IJ08] S. Ionica & A. Joux – « Another approach to pairing computation in Edwards coordinates », in *INDOCRYPT 2008*, 2008, `http://eprint.iacr.org/2008/292`, p. 400–413.

[IKO86] T. Ibukiyama, T. Katsura & F. Oort – « Supersingular curves of genus two and class numbers », *Compositio Math.* **57** (1986), no. 2, p. 127–152.

[Jar08] F. Jarvis – « Higher genus arithmetic-geometric means », *Ramanujan J.* **17** (2008), no. 1, p. 1–17.

[Kan97] E. Kani – « The number of curves of genus two with elliptic differentials », *J. Reine Angew. Math.* **485** (1997), p. 93–121.

[Kan06] — , « The number of genus 2 covers of an elliptic curve », *Manuscripta Math.* **121** (2006), no. 1, p. 51–80.

[Kan08] — , « Jacobians isomorphic to a product of two elliptic curves », 2008, `http://www.mast.queensu.ca/~kani/curves.htm`.

[Kat96] P. Katsylo – « Rationality of the moduli variety of curves of genus 3. », *Comment. Math. Helv.* **71** (1996), no. 4, p. 507–524.

[Kle90] F. Klein – « Zur Theorie der Abelschen Funktionen », *Math. Annalen* **36** (1889-90), p. 388–474, =Gesammelte mathematische Abhandlungen, XCVII, 388-474.

[KMS94] V. Kumar Murty & J. Scherk – « Effective versions of the Chebotarev density theorem for function fields », *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), no. 6, p. 523–528.

[Koh96] D. R. Kohel – « Endomorphism rings of elliptic curves over finite fields », Thèse, University of California, Berkeley, 1996.

[Koh08] — , « Complex multiplication and canonical lifts », in *Algebraic geometry and its applications*, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, p. 67–83.

[KTW09] T. Kodama, J. Top & T. Washio – « Maximal hyperelliptic curves of genus three », *Finite Fields Appl.* **15** (2009), no. 3, p. 392–403.

[KW05] K. Koike & A. Weng – « Construction of CM Picard curves », *Math. Comp.* **74** (2005), no. 249, p. 499–518 (electronic).

[Lan83] S. Lang – *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 255, Springer-Verlag, New York, 1983.

[Lan02] — , *Algebra*, troisième éd., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Lau01] K. Lauter – « Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields », *J. Algebraic Geom.* **10** (2001), no. 1, p. 19–36, With an appendix in French by J.-P. Serre.

[Lau02] — , « The maximum or minimum number of rational points on genus three curves over finite fields », *Compositio Math.* **134** (2002), no. 1, p. 87–111, With an appendix by Jean-Pierre Serre.

[Leh05] D. Lehavi – « Any smooth plane quartic can be reconstructed from its bitangents », *Israel J. Math.* **146** (2005), p. 371–379.

[Liu94] Q. Liu – « Conducteur et discriminant minimal de courbes de genre 2 », *Compositio Math.* **94** (1994), no. 1, p. 51–79.

[LL06] R. Lercier & D. Lubicz – « A quasi quadratic time algorithm for hyperelliptic curve point counting », *Ramanujan J.* **12** (2006), no. 3, p. 399–423.

[LMNX02] A. López, D. Maisner, E. Nart & X. Xarles – « Orbits of Galois invariant n-sets of $\mathbb{P}^1$ under the action of PGL_2 », *Finite Fields Appl.* **8** (2002), no. 2, p. 193–206.

[Loc94] P. Lockhart – « On the discriminant of a hyperelliptic curve », *Trans. Amer. Math. Soc.* **342** (1994), no. 2, p. 729–752.

[LR85] H. Lange & W. Ruppert – « Complete systems of addition laws an abelian varieties. », *Invent. Math.* **79** (1985), p. 603–610 (English).

[LST64] J. Lubin, J.-P. Serre & J. Tate – « Elliptic curves and formal groups », 1964, scanned copies available at `http://www.ma.utexas.edu/users/voloch/lst.html`.

[Mai04] D. Maisner – « Superficies abelianas como jacobianas de curvas en cuerpos finitos », Thèse, Universitat Autònoma de Barcelona, 2004.

[Mat58] T. Matsusaka – « On a theorem of Torelli », *Amer. J. Math.* **80** (1958), p. 784–800.

[Maz86] B. Mazur – « Arithmetic on curves », *Bull. Amer. Math. Soc. (N.S.)* **14** (1986), no. 2, p. 207–259.

[Mea08] S. Meagher – « Twists of genus 3 and their jacobians », Thèse, Rijksuniversiteit Groningen, 2008.

[Mes] J.-F. Mestre – « Courbes de genre 3 avec S_3 comme groupe d'automorphismes », en préparation.

[Mes91a] — , « Construction de courbes de genre 2 à partir de leurs modules », in *Effective methods in algebraic geometry* (Boston), Prog. Math., vol. 94, Birkäuser, 1991, p. 313–334.

[Mes91b] — , « Moyenne de Borchardt et intégrales elliptiques », *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), no. 5, p. 273–276.

[Mil86] — , « Abelian varieties », in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986, p. 103–150.

[Mil04] V. S. Miller – « The Weil pairing, and its efficient calculation », *Journal of Cryptology* **17** (2004), p. 235–261.

[MN02] D. Maisner & E. Nart – « Abelian surfaces over finite fields as jacobians », *Experimental Math.* **11** (2002), p. 321–337, with an appendix of E.W. Howe.

[MN07] — , « Zeta functions of supersingular curves of genus 2 », *Canad. J. Math.* **59** (2007), no. 2, p. 372–392.

[MN08] R. Martí & E. Nart – « Orbits of rational n-sets of projective spaces under the action of the linear group. », *J. Comb. Theory, Ser. A* **115** (2008), no. 4, p. 547–568.

[Mor09] F. Morain – « Edwards curves and CM curves », 2009, `http://arxiv.org/abs/0904.2243`.

[MSSV02] K. Magaard, T. Shaska, S. Shpectorov & H. Völklein – « The locus of curves with prescribed automorphism group », *Sūrikaisekikenkyūsho Kōkyūroku* (2002), no. 1267, p. 112–141, Communications in arithmetic fundamental groups (Kyoto, 1999/2001).

[Mum07] D. Mumford – *Tata lectures on theta. II : Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman, and H. Umemura. Reprint of the 1984 edition.*, Modern Birkhäuser Classics. Basel : Birkhäuser. xiv, 272 p. EUR 34.90/net ; SFR 59.90 , 2007.

[Mum08] — , *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay, 2008, With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[MV05] G. McGuire & J. F. Voloch – « Weights in codes and genus 2 curves », *Proc. Amer. Math. Soc.* **133** (2005), no. 8, p. 2429–2437 (electronic).

[MY00] K. Miura & H. Yoshihara – « Field theory for function fields of plane quartic curves », *J. of Algebra* **226** (2000), p. 283–294.

[Nar09] E. Nart – « Counting hyperelliptic curves. », *Adv. Math.* **221** (2009), no. 3, p. 774–787.

[NS04] E. Nart & D. Sadornil – « Hyperelliptic curves of genus three over finite fields of characteristic two », *Finite Fields and Their Applications* **10** (2004), p. 198–220.

[OMNS08] L. H. O'Connor, G. McGuire, M. Naehrig & M. Streng – « CM construction of genus 2 curves with p-rank 1 », 2008.

[Oor75] F. Oort – « Which abelian surfaces are products of elliptic curves ? », *Math. Ann.* **214** (1975), p. 35–47.

[Oor91a] — , « Hyperelliptic supersingular curves », in *Arithmetic Algebraic Geometry (Texel, 1989)* (Boston), Prog. Math., Birkäuser, 1991, p. 247–284.

[OU73] F. Oort & K. Ueno – « Principally polarized abelian varieties of dimension two or three are Jacobian varieties », *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **20** (1973), p. 377–381.

[Oyo09] R. Oyono – « Non-hyperelliptic modular Jacobians of dimension 3 », *Math. Comp.* **78** (2009), no. 266, p. 1173–1191.

[Rec93] S. Recillas – « Symmetric cubic surfaces and curves of genus 3 and 4 », *Boll. Un. Mat. Ital. B (7)* **7** (1993), no. 4, p. 787–819.

[RF74] H. E. Rauch & H. M. Farkas – *Theta functions with applications to Riemann surfaces*, The Williams & Wilkins Co., Baltimore, Md., 1974.

[Rie76] B. Riemann – « Zur Theorie der Abelschen Funktionen für den Fall $p = 3$ », 1876.

[Roq70] P. Roquette – « Abschätzung der Automorphismenanzahl von Funktionenkörpern », *Math. Z.* **117** (1970), p. 157–163.

[RS02] K. Rubin & A. Silverberg – « Supersingular abelian varieties in cryptology », in *Advances in cryptology—CRYPTO 2002*, Lecture Notes in Comput. Sci., vol. 2442, Springer, Berlin, 2002, p. 336–353.

[Rüc90] H.-G. Rück – « Abelian surfaces and Jacobian varieties over finite fields », *Compositio Math.* **76** (1990), no. 3, p. 351–366.

[Ryb08] S. Y. Rybakov – « Zeta functions of algebraic surfaces and Jacobians of genus 3 curves over finite fields », Thèse, Moscow State University, Mechanics and Math. Department, 2008, en russe, non publiée.

[Sai89] T. Saito – « The discriminants of curves of genus 2 », *Compositio Math.* **69** (1989), no. 2, p. 229–240.

[Sal65] G. Salmon – *A treatise on the analytic geometry of three dimensions. Vol. II*, Fifth edition. Edited by Reginald A. P. Rogers, Chelsea Publishing Co., New York, 1965.

[SB08] N. Shepherd-Barron – « Thomae's formulae for non-hyperelliptic curves and spinorial square roots of theta-constants on the moduli space of curves », 2008, `http://www.citebase.org/abstract?id=oai:arXiv.org:0802.3014`.

[Sch95] R. Schoof – « Counting points on elliptic curves over finite fields », *J. Théor. Nombres Bordeaux* **7** (1995), no. 1, p. 219–254, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Sch98] A. Schiemann – « Classification of Hermitian forms with the neighbour method », *J. Symbolic Comput.* **26** (1998), no. 4, p. 487–508, tables disponibles sur `http://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/`.

[Sek85] T. Sekiguchi – « Wild ramification of moduli spaces for curves or for abelian varieties », *Compositio Math.* **54** (1985), p. 33–372.

[Sek86] — , « Erratum : "On the fields of rationality for curves and for their Jacobian varieties" [Nagoya Math. J. **88** (1982), 197–212 ; MR0683250 (85a :14021)] », *Nagoya Math. J.* **103** (1986), p. 163.

[Ser68] J.-P. Serre – *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser77] — , *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977, Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Ser83] — , « Nombres de points des courbes algébriques sur $\mathbf{F}_q$ », in *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, Univ. Bordeaux I, Talence, 1983, p. Exp. No. 22, 8.

[Ser85] — , « Rational points on curves over finite fields », 1985, Lectures given at Harvard, notes by F.Q. Gouvéa.

[Ser94] — , *Cohomologie galoisienne*, fifth éd., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994.

[Sha03] T. Shaska – « Computational aspects of hyperelliptic curves », in *Computer mathematics*, Lecture Notes Ser. Comput., vol. 10, World Sci. Publ., River Edge, NJ, 2003, p. 248–257.

[Shi67] T. Shioda – « On the graded ring of invariants of binary octavics », *American J. of Math.* **89** (1967), no. 4, p. 1022–1046.

[Sil92] J. H. Silverman – *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Smi08] B. Smith – « Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves », in *Advances in Cryptology : EUROCRYPT 2008, Istanbul* (Berlin), vol. 4965, Springer, 2008, p. 163–180.

[Spa94] A.-M. Spallek – « Kurven vom Geschlecht 2 und ihre Anwendung in Publik-Key-Kryptosystemen », Thèse, Institut für Experimentelle Mathematik, Essen, 1994.

[Sti93] H. Stichtenoth – *Algebraic function fields and codes*, Lectures Notes in Mathematics, no. 314, Springer-Verlag, 1993.

[Str09] M. Streng – « Computing igusa class polynomials », 2009.

[Sub75] D. Subrao – « The p-rank of Artin-Schreier curves », *Manuscripta Math.* **16** (1975), p. 169–193.

[SV86] K.-O. Stöhr & J. F. Voloch – « Weierstrass points and curves over finite fields », *Proc. London Math. Soc. (3)* **52** (1986), no. 1, p. 1–19.

[SV87] — , « A formula for the cartier operator on plane algebraic curves », *J. für die Reine und Ang. Math.* **377** (1987), p. 49–64.

[SV04] T. Shaska & H. Völklein – « Elliptic subfields and automorphisms of genus 2 function fields », in *Arithmetic and geometry with applications (West Lafayette, IN, 2000)* (Berlin), Springer, 2004, p. 703–723.

[Tak08] K. Takashima – « Efficiently computable distorsion maps for supersingular curves », in *ANTS VIII*, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, p. 88–101.

[Tat66] J. Tate – « Endomorphisms of abelian varieties over finite fields », *Invent. Math.* **2** (1966), p. 134–144.

[Tat71] — , « Classes d'isogénie des variétés abéliennes sur un corps fini (d'après Honda) », in *Séminaire Bourbaki 1968/69*, Lecture Notes in Math., vol. 179, Springer, Berlin, 1971, p. 95–110.

[Top03] J. Top – « Curves of genus 3 over small finite fields », *Indag. Math. (N.S.)* **14** (2003), no. 2, p. 275–283.

[Tor00] F. Torres – « The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs », Available on `http://arxiv.org/abs/math.AG/0011091`, 2000.

[Tsu86] S. Tsuyumine – « On Siegel modular forms of degree three », *Amer. J. Math.* **108** (1986), no. 4, p. 755–862.

[Tsu91] — , « Thetanullwerte on a moduli space of curves and hyperelliptic loci », *Math. Z.* **207** (1991), no. 4, p. 539–568.

[Ünv04] S. Ünver – « An Arakelov theoretic proof of the equality of conductor and discriminant », *J. Théor. Nombres Bordeaux* **16** (2004), no. 2, p. 423–427.

[Uzu10] O. Uzunkol – « Konstruktion algebraischer Kurven mittels komplexer Multiplikation nebst Anwendung », Thèse, Technische Universität, Berlin, 2010, en préparation.

[vdG08] G. van der Geer – « Siegel modular forms and their applications », in *The 1-2-3 of modular forms*, Universitext, Springer, Berlin, 2008, p. 181–245.

[vdGvdV] G. van der Geer & M. van der Vlugt – « tables of curves with many points », `http://www.science.uva.nl/~geer/`.

[vdGvdV92a] — , « Reed-müller codes and supersingular curves I », *Compos. Math.* **84** (1992), p. 333–367.

[vdGvdV92b] — , « Supersingular curves of genus 2 over finite fields of characteristic 2 », *Mathematische Nachrichten* **159** (1992), p. 73–81.

[Ver83] A. Vermeulen – « Weierstrass points of weight two on curves of genus three », Thèse, university of Amsterdam, Amsterdam, 1983.

[Ver01] E. R. Verheul – « Evidence that XTR is more secure than supersingular elliptic curve cryptosystems », in *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, Lecture Notes in Comput. Sci., vol. 2045, Springer, Berlin, 2001, p. 195–210.

[Ver03] F. Vercauteren – « Computing zeta functions of curves over finite fields », Thèse, Katholieke Universiteit Leuven, 2003.

[VlT05] P. Viana & O. P. la Torre – « Curves of genus three in characteristic two », *Comm. Algebra* **33** (2005), no. 11, p. 4291–4302.

[vW99] P. van Wamelen – « Examples of genus two CM curves defined over the rationals », *Math. Comp.* **68** (1999), no. 225, p. 307–320.

[Wal95] C. Wall – « Quartic curves in characteristic 2 », *Math. Proc. Cambridge Phil. Soc.* **117** (1995), p. 393–414.

[Wat69] W. C. Waterhouse – « Abelian varieties over finite fields », *Ann. Sci. École Norm. Sup. (4)* **2** (1969), p. 521–560.

[Web76] H. Weber – « Theory of abelian functions of genus 3. (Theorie der Abel'schen Functionen vom Geschlecht 3.) », 1876.

[Wen01] A. Weng – « A class of hyperelliptic CM-curves of genus three », *J. Ramanujan Math. Soc.* **16** (2001), no. 4, p. 339–372.

[Wen03] — , « Constructing hyperelliptic curves of genus 2 suitable for cryptography », *Math. Comp.* **72** (2003), no. 241, p. 435–458 (electronic).

[WM71] W. Waterhouse & J. Milne – « Abelian varieties over finite fields. », 1969 Number Theory Institute, Proc. Sympos. Pure Math. 20, 53-64, 1971.

[Xin94] C. Xing – « The characteristic polynomials of abelian varieties of dimensions three and four over finite fields », *Sci. China Ser. A* **37** (1994), no. 2, p. 147–150.

[Xin96] — , « On supersingular abelian varieties of dimension two over finite fields », *Finite Fields Appl.* **2** (1996), no. 4, p. 407–421.

[Yan07] T. Yang – « Arithmetic intersection on a Hilbert modular surface and the Faltings height », 2007, `http://www.math.wisc.edu/~thyang/RecentPreprint.html`.